KOBIL Smart Key V3.0
User's Guide

August 15th, 2006
English Version

Contents

1 What is KOBIL Smart Key? 3
- 1.1 About KOBIL Smart Key . . . 3
- 1.2 Advantages in your daily Life . . . 3

2 Installation 5
- 2.1 System Requirements . . . 5
- 2.2 Installation . . . 7
  - 2.2.1 Smart Card Reader Drivers . . . 7
  - 2.2.2 CD Setup for Microsoft Windows . . . 7
  - 2.2.3 CD setup for Linux and Solaris . . . 11

3 First Steps 12
- 3.1 Your personal Smart Card . . . 12
- 3.2 Defining the Card PIN . . . 13
- 3.3 Entering the card PIN . . . 14
- 3.4 Certificate Slots on your smart card . . . 15
- 3.5 Where do I get my certificate from? . . . 16

4 Using KOBIL Smart Key for Microsoft Applications 17
- 4.1 Certificate Management . . . 17
  - 4.1.1 You have already a personalized Smart Card . . . 17
  - 4.1.2 Obtaining your Certificate . . . 18
  - 4.1.3 The Windows Certificate Manager . . . 19
  - 4.1.4 Importing a CA Certificate . . . 21
  - 4.1.5 Importing another User's Certificate . . . 22
- 4.2 Securing Internet Web Access using Internet Explorer . . . 23
- 4.3 Secure E-mail Communication using Microsoft Outlook . . . 27
  - 4.3.1 Choose your Certificate . . . 27
  - 4.3.2 Sending secure E-mail . . . 33
  - 4.3.3 Receiving secure E-mail . . . 34
- 4.4 File Security . . . 35
  - 4.4.1 Additional Decryption Keys . . . 35
  - 4.4.2 File Encryption . . . 35
  - 4.4.3 File Decryption . . . 38
  - 4.4.4 Directory Encryption . . . 40
  - 4.4.5 Directory Decryption . . . 40
  - 4.4.6 File Signature . . . 41
  - 4.4.7 File Signature Verification . . . 43
  - 4.4.8 Directory Signature . . . 45
  - 4.4.9 Directory Signature Verification . . . 46
  - 4.4.10 Signature and Encryption of Files and Directories . . . 46
  - 4.4.11 Signature Verification and Decryption of Files and Directories . . . 49

4.5 The CardManagement Tool . . . 51
4.5.1 Registering certificates for the Windows Certificate Manager . . . 52
4.5.2 Deletion of Certificates from your smart card . . . 53
4.5.3 Importing Certificates onto your smart card . . . 53
4.5.4 Change / Unblock tge PIN of your Smart Card . . . 54
4.5.5 Default Settings for File Security . . . 55

5 Smart card Logon for Windows 2000/XP 58
5.1 Prerequisites . . . 58
5.2 Enrollment Agent Certificate . . . 59
5.3 Issuing Smart Card Logon Certificates . . . 62
5.4 The Smart Card Logon Process . . . 65
5.5 Important notes about Windows 2000 / XP Smartcard Logon . . . 66
5.6 Smart Card Logon for Terminal Server Environments . . . 67

6 Using the KOBIL Smart Key PKCS#11 Module for Netscape 68
6.1 Certificate Management with Netscape . . . 68
6.1.1 Getting your Certificate . . . 68
6.1.2 Managing Certificates . . . 72
6.1.3 Importing a new CA Certificate . . . 76
6.1.4 Importing another User's Certificate . . . 76
6.1.5 Importing a Web Server's Certificate . . . 77
6.1.6 Changing the PIN of your TCOS Smart Card . . . 77
6.2 Secure Web Sessions using Netscape Navigator . . . 77
6.3 Secure E-mail Communication using Netscape Messenger . . . 81
6.3.1 Choose your Certificate . . . 81
6.3.2 Sending secure E-Mail . . . 83
6.3.3 Receiving secure E-Mail . . . 83

A Problems and Solutions 85
A.1 Connecting the chipcard terminal . . . 85
A.2 KOBIL Smart Key for Microsoft-Applications . . . 85
A.3 KOBIL Smart Key PKCS#11 module for Netscape . . . 86

B Cryptographic Basics and Standards 87
B.1 Security Objectives . . . 87
B.2 Terms and Basics . . . 87
B.3 Standards . . . 88
B.3.1 Data Digestion Algorithms . . . 88
B.3.2 Symmetric Encryption Algorithms . . . 88
B.3.3 Public Key Algorithms . . . 89
B.3.4 Digital Certificates . . . 94
B.3.5 Certificate Authorities . . . 95
B.3.6 Smart Cards and Readers . . . 96
B.3.7 Secure Socket Layer(SSL) . . . 96
B.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME) . . . 97

C Glossary 100

Chapter 1

What is KOBIL Smart Key?

1.1 About KOBIL Smart Key

KOBIL Smart Key secures e-mail communications and web sessions by way of smart cards. Moreover, it offers smart card based file encryption and signature on Windows systems as well smart card logon for Windows 2000 and XP systems.

KOBIL Smart Key consists of a smart card and a KOBIL reader as hardware modules and plug-ins for some common web browsers, e-mail programs and Windows Explorer as software modules. KOBIL Smart Key puts forward a solution based on Public Key Infrastructure (PKI) and smart card technology which provide hardware based security.

PKI provides the infrastructure needed to implement mechanisms realizing privacy, integrity, and authentication functionalities. The key component of a PKI is the usage of certificates by all connected users and servers. A certificate is a digital identity that holds the owners public information and necessary cryptographic keys. Certificates and the corresponding private keys are are valid for a predefined period. The private keys must be kept secure and used only by their owners. If private keys are stored on a hard drive or a floppy disk, they are susceptible to modification and usage by malicious people. This is a security hole for PKI that can be closed by using smart cards as a secure storage media.

Smart cards are credit card sized devices with integrated circuit chips (ICC) on them. They have their own security mechanisms to lock themselves against physical, electrical and chemical attacks. When private keys are loaded, they never leave smart card and a PIN ("Personal Identification Number") code protects the key usage. Smart cards are easy to use. They fit in any wallet and thus can be easily carried.

KOBIL Smart Key combines the privacy, integrity, and authentication functionalities of PKI with the simplicity, mobility and hardware based security features of smart cards. For the most up-to-date information about the KOBIL Smart Key and related security products, please see the product information page online at *www.kobil.com*.

1.2 Advantages in your daily Life

You can use KOBIL Smart Key together with your favourite web browsers (Internet Explorer and Netscape Communicator), e-mail programs (Outlook Express, Outlook and Netscape Messenger) and with the Windows Explorer. These applications have some built-in features to support the latest industry standards such as SSLv3 (for secure web access) and S/MIME (for secure e-mail) that enable interoperability of security services between different platforms both on client and servers.

With KOBIL Smart Key, you can load your private keys and certificates into your smart card and use them from any computer at home, at work or at any public place like Internet cafes. Your private information will always be kept in your Smart Card. If you lose your card and a malicious person finds it, your card will be locked after three wrong trials.

If a malicious person finds out the password of your e-mail account or he/she logs on your computer, he can read your e-mails and send e-mails from your account to other people. By using KOBIL Smart Key, your e-mails will be kept encrypted and your outgoing e- mails will be approved by a digital signature. Someone should hold your smart card with the knowledge of its PIN to break the encrypted e-mails or to mimic your identity to e-mail recipients.

Secure web connections are needed for many applications (like home banking, e-commerce, digital government etc.) whenever you need to prove your identity and/or hide all sent and received private information, such as credit card numbers. You can easily carry your KOBIL Smart Card in your wallet and use it to authenticate yourself and to protect your private information in the Internet.

KOBIL Smart Key enables you to encrypt your private files and sign them digitally on Windows based systems. KOBIL Smart Key also can be used for smart card based Windows 2000/XP domain logon.

Chapter 2

Installation

2.1 System Requirements

- Microsoft Windows XP (at least Service Pack 1) or
  Microsoft Windows 2000 (at least Service Pack 2) or
  Microsoft Windows Server 2003
  Microsoft Windows 98SE / Me
  Microsoft Windows NT4 (Service Pack 6)
  (optional) Linux with glibc-2.1.3 (for example SuSE Linux 7.2)
  (optional) SUN Solaris Version 2.7

- Supported Software:
  Microsoft Office 2003
  Microsoft Office xp
  Microsoft Outlook 2000 SR-1
  Microsoft Outlook 98
  Microsoft Outlook Express at least Version 5
  Microsoft Internet Explorer at least Version 5.5
  Netscape Communicator at least Version 4.04[1]
  Mozilla at least Version 1.4
  Firefox at least Version 1.0

- Supported Smartcards: T-Telesec TCOS 2.02 / 2.03 min
  T-Telesec TCOS 3.0 Netkey
  T-Telesec E4 Netkey / Netkey 2000
  Siemens CardOS M4.0 / M4.01 / M4.01a / M4.2 / M4.3b
  GemXPresso JavaCard
  IBM JCOP JavaCard

- Hardware:
  128 MB RAM
  20 MB free hard disk space
  CD-ROM or DVD-ROM drive
  A KOBIL Smartcard Terminal

[1] Please note that Netscape supports strong cryptography starting with version 4.73

The seperate **KOBIL Smart Key SigG-CSP** allows working with qualified signatures according to the European Signature Act using E4 Netkey smartcards.

2.2 Installation

2.2.1 Smart Card Reader Drivers

Please install first the smart card reader drivers by following the instructions shipped with your smart card reader.

KOBIL Smart Key supports both PC/SC and CT-API driver models. On Windows, PC/SC is strongly recommended to enable full functionality.

If you like to use a third-party smart card reader, please contact your local KOBIL partner or KOBIL directly.

2.2.2 CD Setup for Microsoft Windows

1. Quit all running programs
2. Insert your KOBIL Smart Key CD-ROM into your CD-ROM/DVD-ROM drive. The installation routine should start automatically. If this is not the case, please click on Start - Execute and enter **D:\Setup.exe** (replace *D* by your CD-ROM's drive letter)

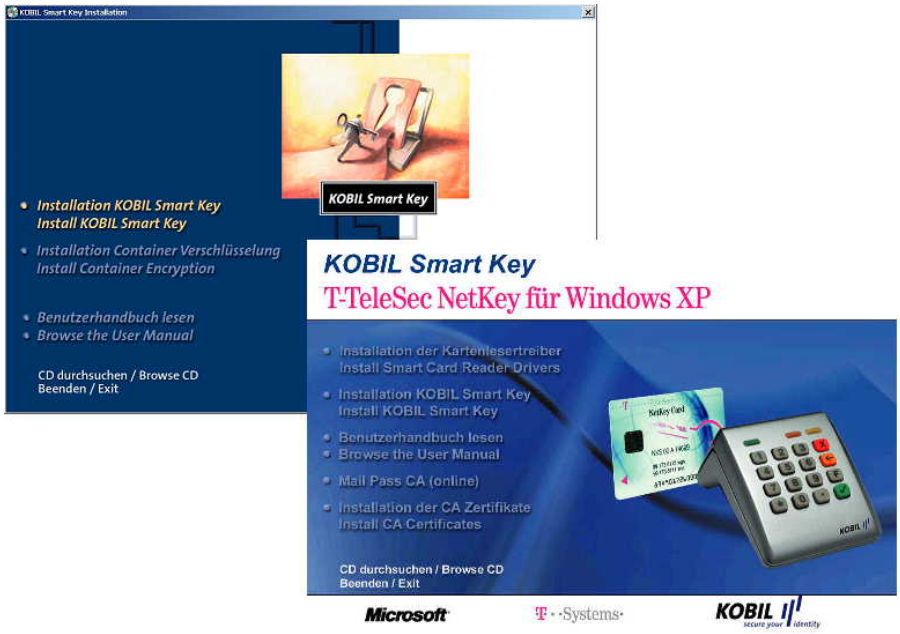

Figure 2.1: CD-ROM start screen

3. Now choose *Install KOBIL Smart Key*

4. You are asked for the setup language.

Wählen Sie eine Setup-Sprache aus
Wählen Sie die Sprache dieser Installation aus der unten aufgeführten Auswahl aus.
Englisch
OK
Abbrechen

Figure 2.2: Selecting the setup language

5. You must agree to the licence agreement to continue installation.

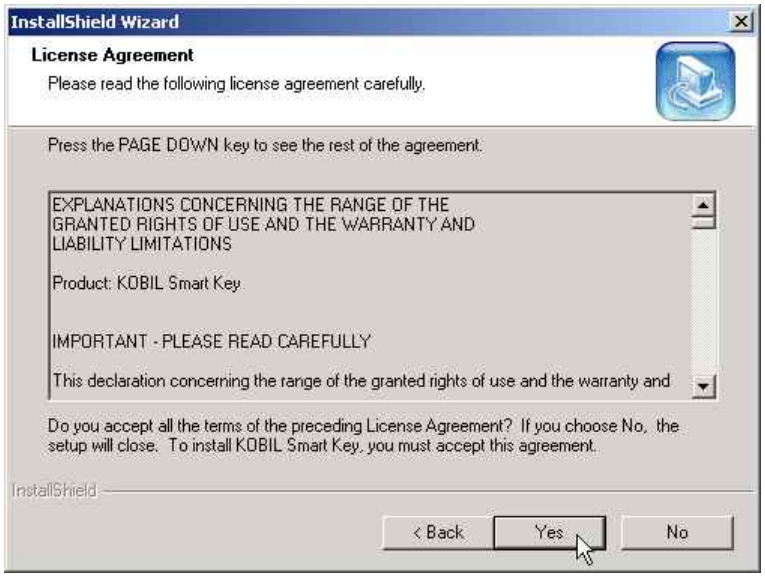
InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
EXPLANATIONS CONCERNING THE RANGE OF THE GRANTED RIGHTS OF USE AND THE WARRANTY AND LIABILITY LIMITATIONS
Product: KOBIL Smart Key
IMPORTANT - PLEASE READ CAREFULLY
This declaration concerning the range of the granted rights of use and the warranty and
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install KOBIL Smart Key, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 2.3: Licence Agreement

6. Enter the destination directory path for the KOBIL Smart Key program files. By default, this is **C:\Program Files \KOBIL Systems\KOBIL Smart Key**. Click on **Browse** to select another path.

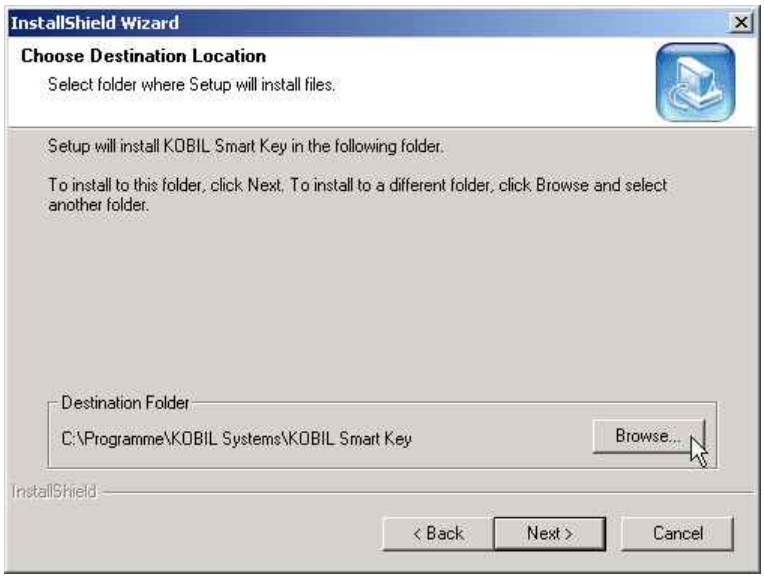
InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install KOBIL Smart Key in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Programme\KOBIL Systems\KOBIL Smart Key
Browse...
InstallShield
< Back
Next >
Cancel

Figure 2.4: Selecting the destination directory

7. Now, you can select the program group. In most cases, you simply can use the default which is *KOBIL Systems*. The program group will appear in the start menu.

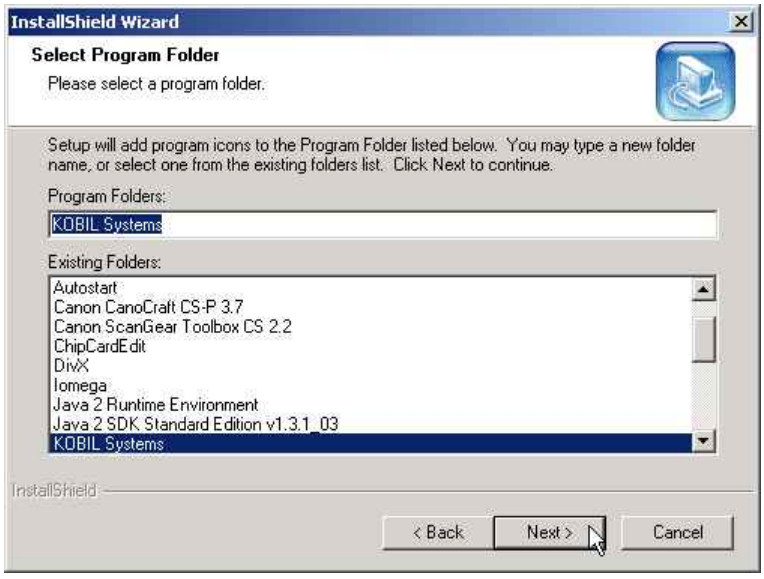
InstallShield Wizard
Select Program Folder
Please select a program folder.
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.
Program Folders:
KOBIL Systems
Existing Folders:
Autostart
Canon CanoCraft CS-P 3.7
Canon ScanGear Toolbox CS 2.2
ChipCardEdit
DivX
Iomega
Java 2 Runtime Environment
Java 2 SDK Standard Edition v1.3.1_03
KOBIL Systems
InstallShield
< Back
Next >
Cancel

Figure 2.5: Program Group

8. Now, you can check the connection to the smart card reader. For terminal server installations, you can skip this test.

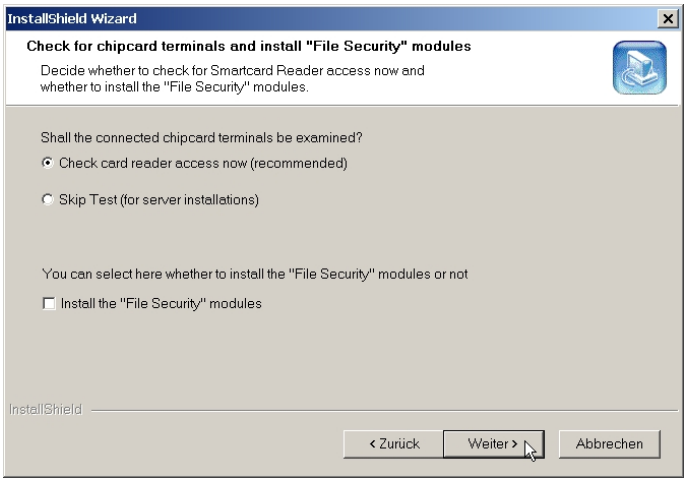
InstallShield Wizard
Check for chipcard terminals and install "File Security" modules
Decide whether to check for Smartcard Reader access now and whether to install the "File Security" modules.
Shall the connected chipcard terminals be examined?
Check card reader access now (recommended)
Skip Test (for server installations)
You can select here whether to install the "File Security" modules or not
Install the "File Security" modules
InstallShield
< Zurück
Weiter >
Abbrechen

Figure 2.6: Smart Card Reader conntection check

If you want to use the file security functionality (see section 4.4), please select the option **Install the file security modules** here.

2.2.3 CD setup for Linux and Solaris

Note that PKCS#11 support for Linux and Solaris is not included in all versions of KOBIL Smart Key.

On an **Linux or Solaris system**, proceed as follows:

1. Insert the KOBIL Smart Key CD-ROM into your CD-ROM drive. On Linux or Solaris systems, mount the CD-ROM with permissions for executing programs, i.e. type

   mount -o exec /cdrom

   at the command-prompt.

2. Change to the CD-ROM's root directory and start the installation script

   install_linux_solaris.sh

3. Select the KOBIL Reader for which you want to install the CTAPI driver. Select an (existing) installation directory for the driver's shared object or DLL and select an installation directory for the PKCS#11 module (for the later, you can simply press **Enter** if you want to have it installed in the same directory as the driver). Both directories should be included in the list of directories searched for shared objects, e.g. on a Linux or Solaris system, they could be included in **LD_LIBRARY_PATH**, on OS/2, they need to be included in the **LIBPATH** statement in **config.sys**.

4. Add the new PKCS#11 module to your Netscape configuration. In order to do this, we provided the file **PKCS11-Install.html** which manages the installation if JavaScript is enabled. Generally, we suggest to disable JavaScript for security reasons, however it is safe to enable it for processing this page. Note that for the user executing the installation, Netscape is started automatically and displays this page. However all other users need to do that step of the installation on their own - you might want to copy that file to some location accessible to everyone.

Chapter 3

First Steps

3.1 Your personal Smart Card

Figure 3.1: Your personal Smart Card

Figure 3.1 shows your personal smart card. It contains your private keys and your certificates. Access to the private keys are protected by a PIN (Personal Identification Number) which you can define.

The **Card PIN** protects all certificates except the qualified signature certificate, e.g. certificates for email encryption, VPN authentication, Windows logon or enhanced signatures.

The **E4 Netkey card for qualified signatures** has an additional **Signature PIN** which protects only the certificate for qualified signatures. This requires that you own a qualified certificate according to the European Signature Act. For more information about qualified signatures, please refer to (KOBIL Smart Key SigG-CSP needs to be installed):

Start > Programs > KOBIL Systems > Qualified Signature > User Manual

Depending on the rollout process, your smart card is either in the so-called **Nullpin-State** (which requires that you define your personal PIN before starting to work) or you get a PIN-Letter containing the card's PIN and PUK values. If the card is completely unpersonalized, you will be prompted to define your initial PIN and – depending on the card type – also the PUK to unlock the PIN.

3.2 Defining the Card PIN

If you did not receive a PIN/PUK letter with your card, you will be prompted to define the PIN and – depending on the card type – also the PUK for the card.

The E4 Netkey card is initially in the so-called NULLPIN state which shows that the card had not been used before. You have to define your personal PIN in this case, too.

Figure 3.2: NULLPIN-State of the card PIN (E4 Netkey card only)

You have to enter the **6-digit** card PIN twice for confirmation. For technical reasons, the PIN is entered using the PC's keyboard, even if you have a secure PIN Pad smart card reader.

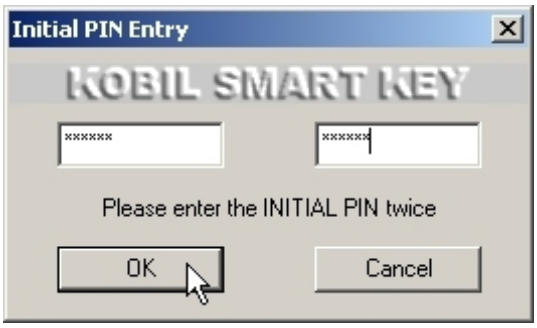

Figure 3.3: Definition of the card PIN

Figure 3.4: NULLPIN has been broken, card PIN is defined (E4 Netkey card only)

For all unpersonalized cards except the E4 Netkey card, you will be prompted to define the PUK and the card PIN. The PUK can be used to unlock the PIN in case it is locked.

For E4 Netkey cards, you can not define the PUK by yourself, because the card already has an encrypted PUK. You can read it out using the CardManagement Tool.

3.3 Entering the card PIN

Whenever the card PIN is required, a dialog appears that asks you to enter the PIN, depending on your smart card reader type (secure PIN entry or PC keyboard entry):

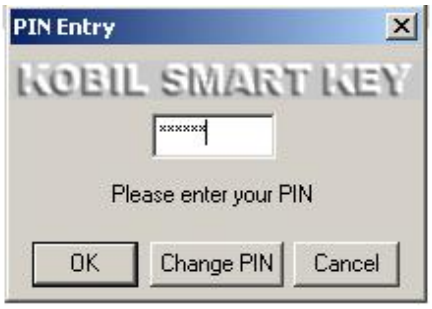

Figure 3.5: PIN entry using the PC keyboard

Figure 3.6: Secure PIN entry using the reader's keyboard

If you enter a wrong card PIN or signature PIN three times subsequently, the PIN is irreversibly locked. So please pay attention before entering the second or third try! If the card PIN has been locked, it can be unlocked by a **PUK** code, similar to mobile phones. For more details about this, please refer to section 4.5.4.

3.4 Certificate Slots on your smart card

Your smart card has several certificate slots where you can store your certificates in. These are in particular:

- Three universal certificates for encryption, authentication and enhanced signatures
- A Windows 2000 / XP logon certificate
- (E4 Netkey card only:) A qualified signature certificate. For more information about qualified signatures, please refer to the separate **KOBIL Smart Key Sigg-CSP** documentation.

The certificate slots are displayed in the CardManagment Tool, as shown in figure 4.33[1]. When you apply for a new certificate, you can select the certificate slot where to put the new certificate (see section 4.1.2).

[1]Note: the qualified signature certificate is not displayed in CardManagement Tool

3.5 Where do I get my certificate from?

By default, your smart card does not contain any certificate, it is empty. This means, you have to apply for a new certificate first. This is necessary, because the Trust Center has to check your identity first in order to issue a high quality certificate.

You have the following possibilities to apply for a certificate:

- Run an **own trust center**(e.g. KOBIL mIDentity Manager or Windows 2000/2003 CA)
- **Third Party certificates** from vendors in the internet: see section 4.1.2
- A **Qualified Signature certificate according to the European Signature Act**: For more information about qualified signatures, please refer to the **KOBIL Smart Key Sigg-CSP** documentation.

Chapter 4

Using KOBIL Smart Key for Microsoft Applications

KOBIL Smart Key for Microsoft applications consists of a so-called *Cryptographic Service Provider* (CSP) for the Microsoft CryptoAPI as well as some tools. This way, all programs compatible with the CryptoAPI – like Internet Explorer or Outlook – work perfectly together with KOBIL Smart Key.

4.1 Certificate Management

KOBIL Smart Key is integrated completely into the Windows certificate management. This chapter therefore explains the usage of the Windows certificate management mechanisms.

First, we must distinguish between two cases:

- **If you have already a personalized smart card**, continue reading section 4.1.1 and skip section 4.1.2. This is the case if you get your smart card from your administrator.
- **If your smart card is still empty**, continue reading section 4.1.2.

4.1.1 You have already a personalized Smart Card

In some applications **you get a completely personalized smart card from your card issuer**, which already contains a certificate. In these cases, you don't have to enroll a certificate, of course. Instead, the certificate on this smart card has to be registered at the Windows certificate manager by means of the CardManagement Tool.

To do this, run once the program Programm

Start > Programs > KOBIL Systems > KOBIL Smart Key > Register Certificates

You will be asked to insert your smart card and to enter the PIN. Then all certificates on your smart card will be registered automatically. See section 4.5 for details.

If you get errors during this step, it may be that your smart card does not contain any certificates yet. In such a case, see section 4.1.2.

4.1.2 Obtaining your Certificate

You'll have to do these steps only if you don't have any certificate on your smart card yet.

1. Install KOBIL Smart Key on your machine (see section 2.2).
2. Insert your smart card into your reader.
3. Run Internet Explorer
4. Surf into your preferred Certificate Authority's web page like
   TeleSec-Trustcenter (Germany): www.telesec.de
   TC Trustcenter (Germany): www.trustcenter.de
   Verisign (USA): www.verisign.com
5. Find the page to get a certificate. You may choose to get a demo certificate.
6. Each CA requires some basic information such as your name and e-mail address.
   Note that if your email address is not entered correctly, you will not be able to process secure email!
7. As Cryptographic Service Provider (CSP), **KOBIL Smart CSP v1.0** must be selected
8. Submit your request. At this point, your keys will be generated and written into your smart card. Your public key and other entries are sent to the CA's server. Depending on your smart card's status, you are either asked to define a PIN for the card (if the card is emtpy) or to enter the card's PIN.

Certificate Enrollment
KOBIL SMART KEY
Status
Available Slots
(Cert Exist) Netkey Enc-Certificate
(Empty) Netkey Enc-Certificate 2
(Empty) Netkey Enc-Certificate 3
(Empty) Netkey Sign-Certificate
(Empty) Windows 2000 Logon-Certificate
Certificate Slot Detail
This slot is empty
Do not unregister old certificate after renewal
Please select a slot to enroll a new certificate
Enroll
Cancel

Figure 4.1: Selecting the Certificate Slot on the Card

Figure 4.1 shows the certificate slot selection dialogue. If allows you to select the certificate slot on the card which the card will be written to. You can decide to use an empty slot (e.g. there will be an additional certificate) or if a already existing slot will be overwritten. Overwriting can be useful to renew an expired certificate.

9. You either will get your certificate immediately on the next page or the CA will explain how to get your certificate. Please follow these instructions.
10. If you have followed the CA's instructions correctly, you should now install your certificate. In most cases, there is a *Install Certificate* button. Your certificate will be written into your smart card and it will be registered on that computer.
11. If you want to use your certificate on other computers (your notebook and PCs at home or at work), please use the CardManagement Tool and your card to register your certificate on those computers (see section 4.5).
12. Take a look at your new certificate using the windows certificate manager as described in section 4.1.3. If your certificate is not valid **because of missing information**, you will have to **import the root certificate** of your Certificate Authority as described in section 4.1.4.

Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.
First Name:
Nickname or middle initial allowed
(example -- Jack B.)
Last Name:
(example -- Doe)
Your E-mail Address:
(example -- jbdoe@verisign.com)
Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID
I'd like a one-year, full-service Digital ID for only US$14.95 per year.
I'd like to test drive a 60-day trial Digital ID for free.
Does not include revocation, replacement, renewal or coverage under the NetSure Protection Plan.
(Optional): Select The Cryptographic Service
If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.
Cryptographic Service Provider Name
Kobil Smart CSP V1.0
Digital ID Subscriber Agreement
You must read this subscriber agreement before applying for, accepting, or using a Digital ID (certificate). If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital ID (certificate).
THIS SUBSCRIBER AGREEMENT will become effective on the date you submit the certificate application to the designated Issuing Authority (IA). By submitting this Subscriber Agreement (and certificate application) you are requesting that the IA issue a Digital ID (certificate) to you and are expressing your agreement to the terms of this Subscriber Agreement. VeriSign's Public Certification Services are governed by VeriSign's Certification Practice Statement (the "CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The CPS is published on the Internet in VeriSign's
Read CPS
Download CPS
If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.
Accept
Decline

Figure 4.2: The Certificate Request Page of VeriSign

4.1.3 The Windows Certificate Manager

The Windows Certificate Manager is Windows' central storage for all certificates. It can be started in three ways:

1. From **Control Panel** using

   Internet Optionen > Content > Certificates

2. From **Internet Explorer** using the pull-down menu

   Extras > Internet Options > Content > Certificates

3. From **Outlook Express** usign the pull-down menu

   Extras > Options > Security > Digital ID's

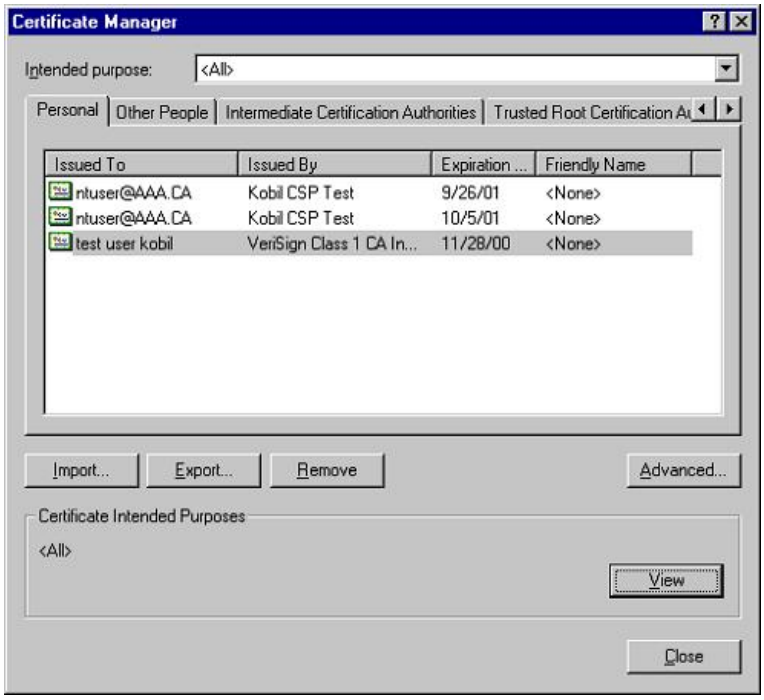

Figure 4.3: The Windows Certificate Manager

You can see the details and the trust path of a certificate from the Certificate dialog. Trust path includes the root and intermediate CA certificates that sign and approve this certificate in an hierarchical order. If any of the certificates in the path is not trusted (its signature is not valid or the root CA is unknown), that certificate and all other certificates below will be marked with a red cross, showing that those certificates can not be used.

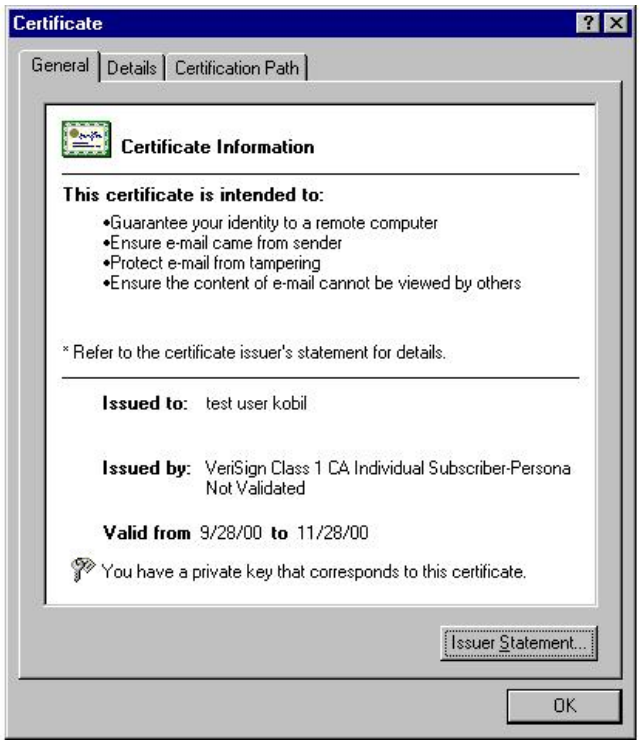
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee your identity to a remote computer
•Ensure e-mail came from sender
•Protect e-mail from tampering
•Ensure the content of e-mail cannot be viewed by others
* Refer to the certificate issuer's statement for details.
Issued to: test user kobil
Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Valid from 9/28/00 to 11/28/00
You have a private key that corresponds to this certificate.
Issuer Statement...
OK

Figure 4.4: Certificate details

The Windows Certificate Manager also allows to export certificates[1] and to delete them. If you delete a certificate in Windows Certificate Manager, the certificate is only **unregistered**, it is not deleted physically on the smart card. You can register the certificate using CardManagement Tool if you unregistered it accidentally. If you want to delete the certificate from the card, use CardManagement Tool (see section 4.5).

4.1.4 Importing a CA Certificate

If you want to do secure communication with users of a new certification authority, you have to import its CA certificate (also called *root certificate*) first. If the CA certificate of a known certification authority expires, you also have to import the new CA certificate.

1. Download the root certificate from the CA's Web site.
2. The certificate will be displayed with the hint that it is **not trusted**, because it is not stored in the **Trusted Root Certification Authorities**.
3. Click on **Install Certificate**.
4. The following dialogues can be skipped using the button *next*.
5. The last dialogue box asks you to confirm the CA certificate's fingerprint. You should obtain this fingerprint on a independent way, for example on the CA's letter paper or on its web pages.

[1] note that the smart card's private key can never exported

Note that you automatically get an implicit trust relationship to all users of the new certification authority when you import its CA certificate! You should inform yourself about the certification poliy of the new certification authority before importing its CA certificate.

After successful import, you find the new CA certificate in the Windows Certificate Manager either in **Intermediate Certification Authorities** or in **Trusted Root Certification Authorities** (see section 4.1.3).

4.1.5 Importing another User's Certificate

Before you can send e-mail to a user, you must get the user's digital certificate and add it to your address book. You can obtain the certificate by two ways:

- Receive a signed e-mail from the user. Signed e-mail contain the user's digital certificate.
- Obtain the user's certificate from a public directory service:

  Outlook Express

  In Outlook Express, choose the menu

  Edit > Find > People

  Outlook 98 / 2000 / xp

  In Outlook, click on **Find People** in the menu

  Extras > Adress Book

  Figure 4.5 shows the dialogue for all Outlook versions. You can search for the recipient's name or e-mail address.

Setting-up a new directory service

If you want to use any other than the pre-installed directory services, open the menu

Extras > Accounts > Directory Service

and click on the button **Add > Directory Service...**. An assistant will be started that will guide you throught the process. You will have to enter the following informations:

- **Directory Server:** This is the address of the new directory server.
- **Authorization Required:** If this checkbox is active, you will have to enter a username and a password for user authentication. Usually, this option is not used.
- **Check Addresses with this Directory Service:** If this checkbox is active, the directory service will be used to resolve e-mail addresses from user names and to search automatically for recipient's certificates.

Once the directory service is configured, it may be necessary to enter the directory service's **Search Base**. To do that, select the newly installed directory service once more and click on **Properties**. In the drawer **Extended** you can enter the **Search Base**.

Ask your system administrator for the parameters suitable for your directory service.

You can also configure a directory service for **automatic Search for certificates** of e-mail recipients by activating in the menu

Extras > Accounts > Directory Service > Properties

tge option **Check recipient addresses with this directory service**.

Once you have successfully imported another user's certificate, you can take a look at it in the Windows certificate manager under **Other People** (see section 4.1.3).

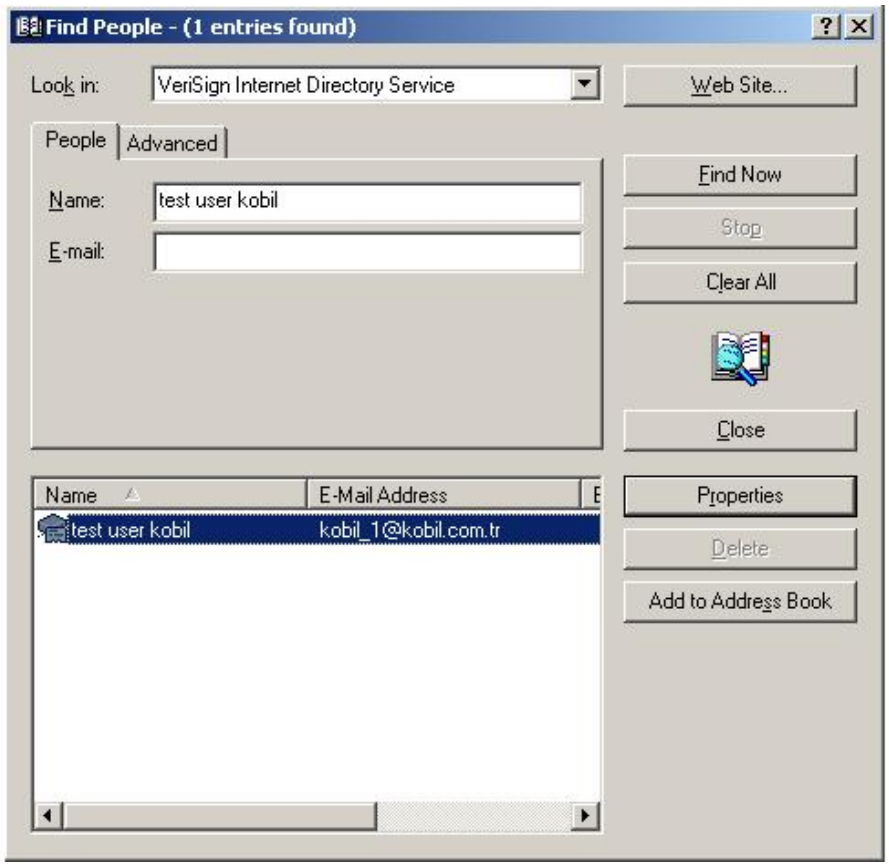

Figure 4.5: Find People Dialog

4.2 Securing Internet Web Access using Internet Explorer

1. When your browser enters a secure site, you will get a security alert, if you did not disable this alert before. You should accept it. You can check the option not to see this warning in the future.

Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info

Figure 4.6: Security Alert

2. Web site response with its certificate. Your browser checks the signature and other properties of this certificate. If the certificate has a security problem, you will get the following security alert.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No
View Certificate

Figure 4.7: Security Alert

3. If the web site wants you to authenticate yourself, you will be prompted with a client authentication dialog that lists all your certificates. If there is no certificate on the list, it means you do not have a certificate for this process. You can select and view any certificate before selecting the proper one. You can also press the **More Info** button to see Internet Explorer Help.

Figure 4.8: Client Authentication

4. If you select a certificate which is loaded by KOBIL Smart Key (or registered by CardManagement Tool) you will be prompted with a PIN entry dialog. Depending on your chipcard terminal, you must enter the PIN either via your computer's keyboard (see figure 4.9) or via the chipcard terminal's keypad (*Secure PIN-entry*, see figure 4.10). You should insert your smart card before proceeding.

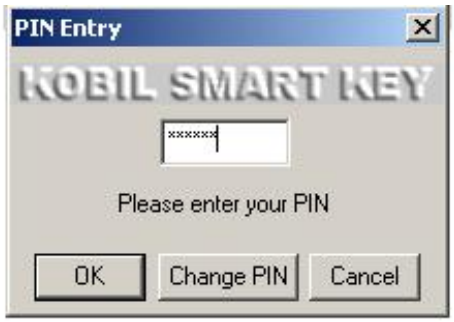

Figure 4.9: PIN Entry Dialog

Figure 4.10: Secure PIN-entry on the smart card terminal

5. After a successful PIN entry, SSL connection will be accomplished. You should see the yellow lock on the status bar of Internet Explorer.

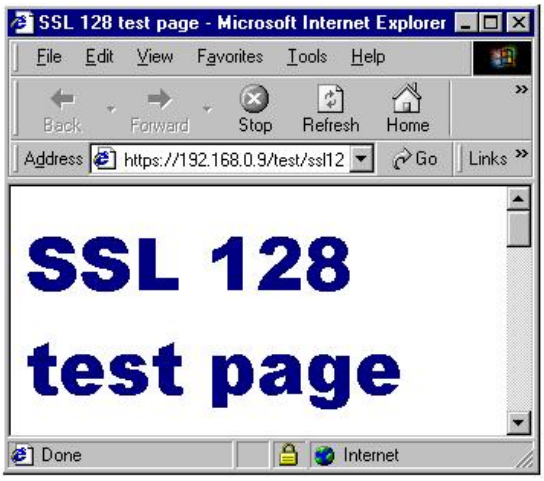

Figure 4.11: Secure Web Page

4.3 Secure E-mail Communication using Microsoft Outlook

In this section, you'll learn how to secure your e-mails using Microsoft Outlook Express, 98 and 2000 with KOBIL Smart Key. **We assume that both your internet access and e-mail account are properly configured. If you are not sure about this, contact your internet provider**.

4.3.1 Choose your Certificate

To send signed messages and receive encrypted messages, you have to configure your e-mail certificate. If you don't select a default certificate and try to send a signed message, Outlook Express prompts you with a list of certificates to choose from.

The necessary steps differ a bit between Outlook Express and Outlook 98/2000

Outlook Express

In Outlook Express, your certificates are bound to your e-mail account, so you can select a default certificate for a each account.

1. Start Outlook Express and select

   Tools > Accounts

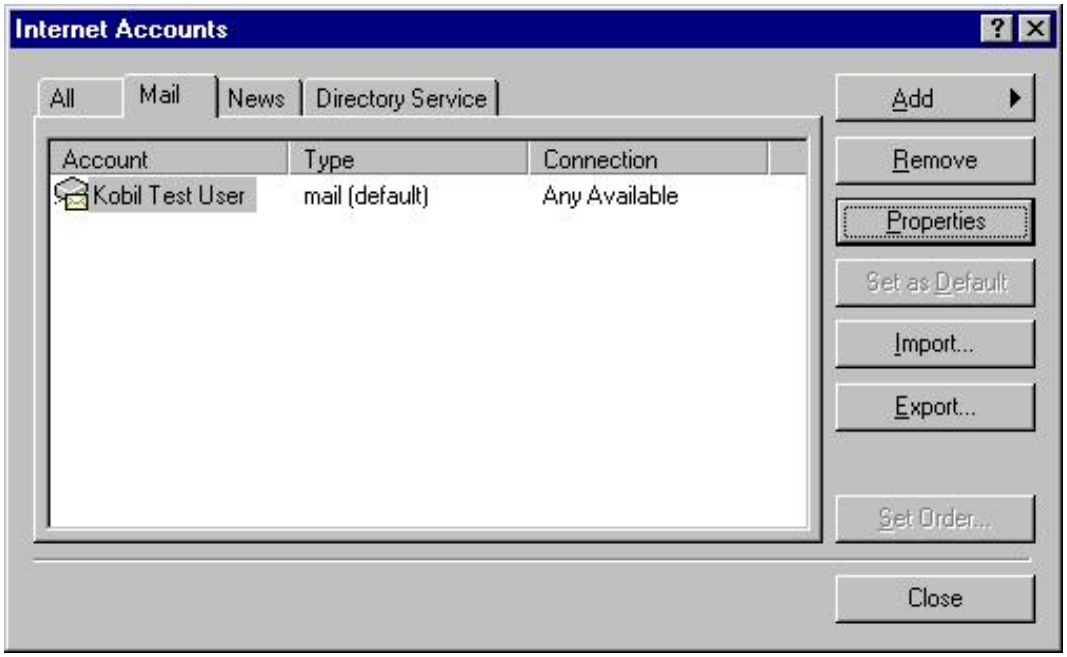

Figure 4.12: Internet Accounts Dialog

2. Choose your e-mail account as shown in figure 4.12 and click

   Properties > Security

   The dialogue shown in figure 4.13 will appear.

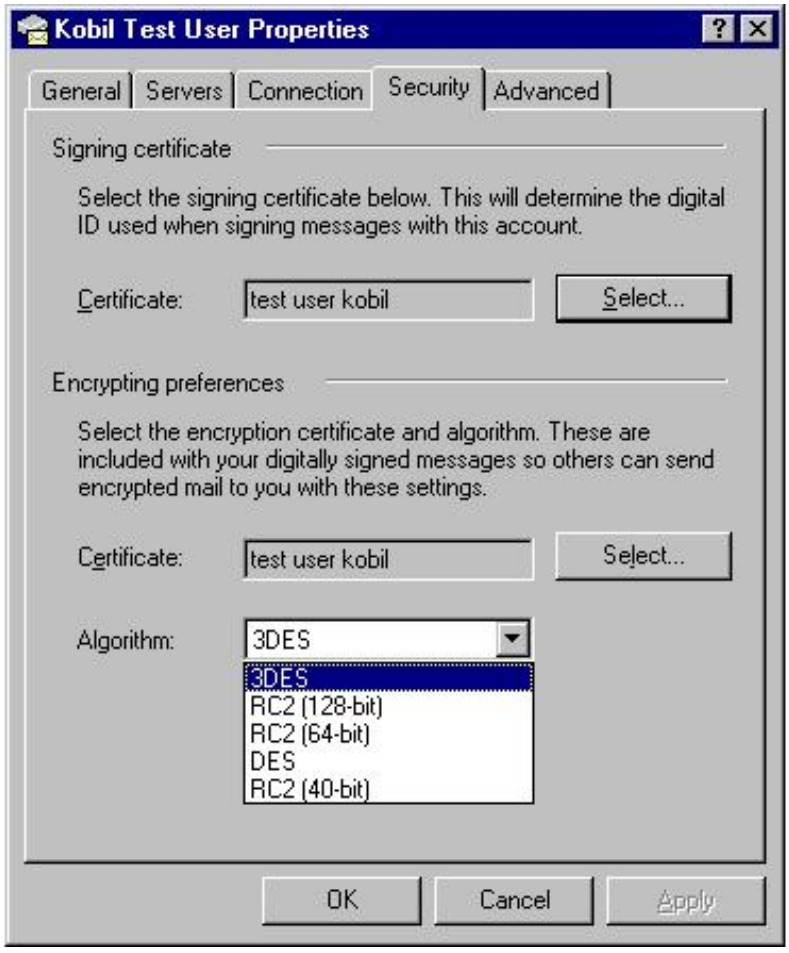

Figure 4.13: Internet Accounts properties Dialog

3. Click **Select** and choose a certificate from the list that shows all the certificates which can be associated with the account you selected above. If there are other certificates which don't have the same e-mail account information, they will not be displayed in this list. You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 4.14.

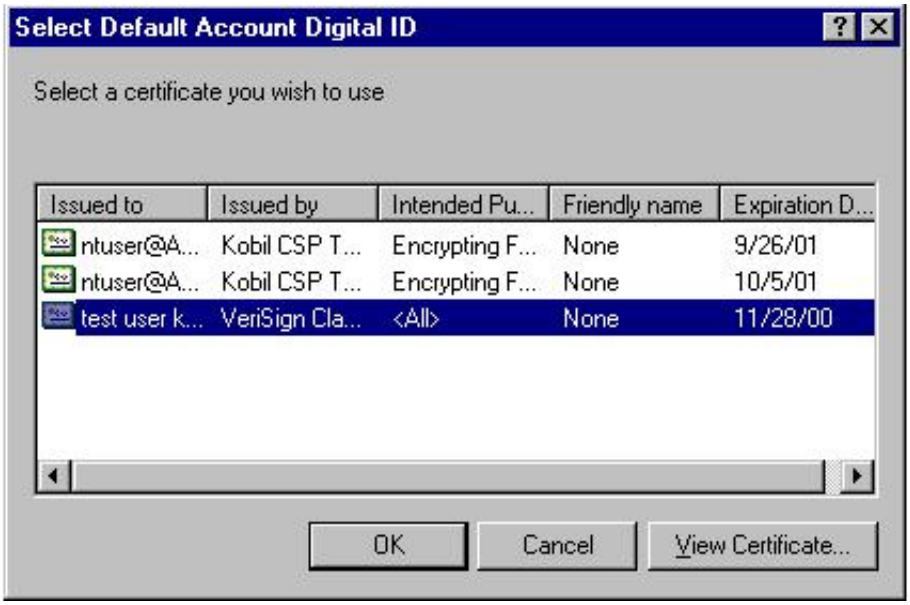

Figure 4.14: Select Digital ID Dialog

4. You can select the session key algorithm which will be used for bulk encryption and decryption. For strongest security, **3DES** or **RC2 128-bit** is recommended.

Outlook 98 / 2000

1. Start your Outlook 98 / 2000 and choose the menu

   Extras > Options

2. Choose the drawer **Security** as shown in figure 4.15.

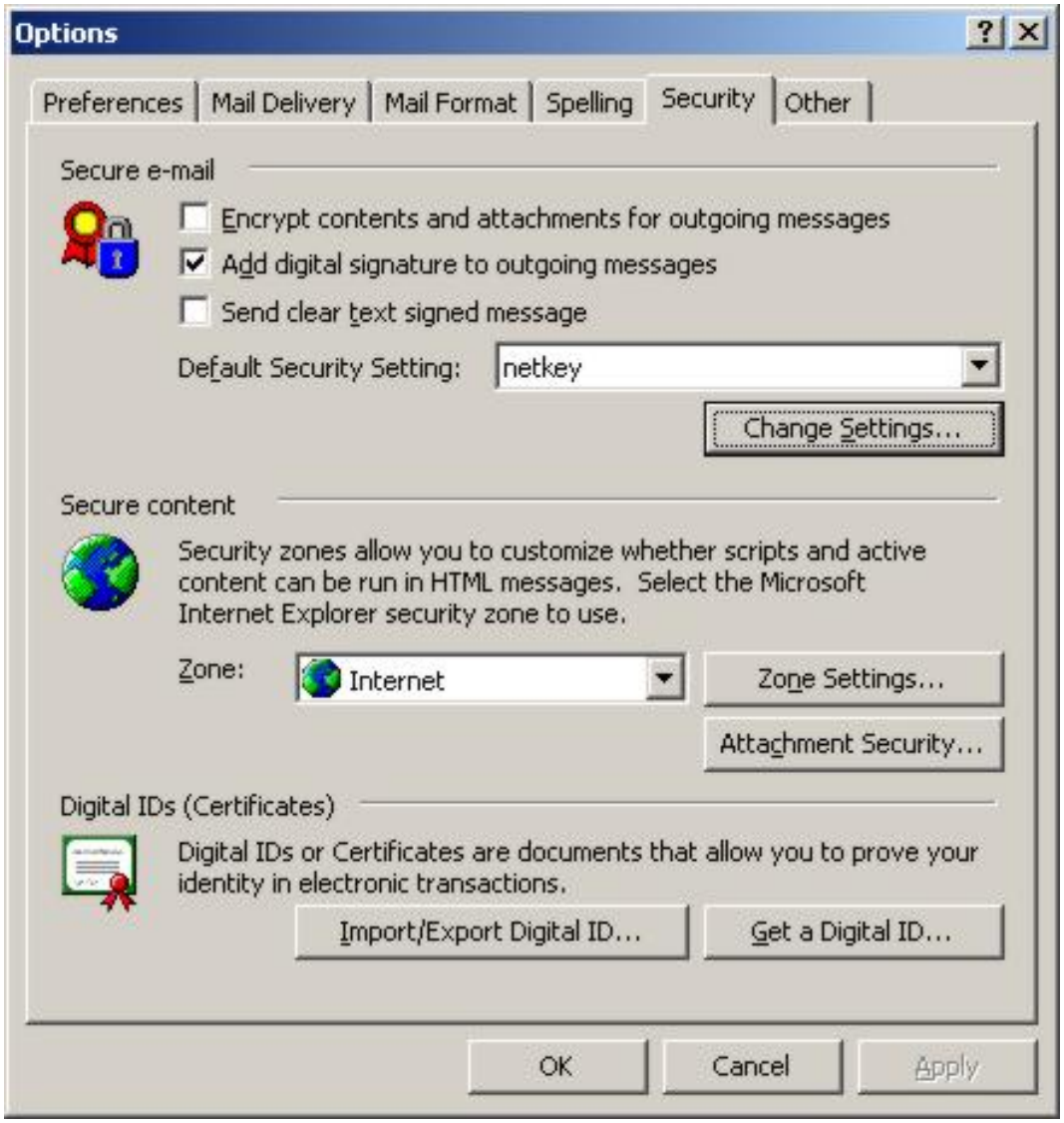

Figure 4.15: Security Options dialogue in Outlook 98 / 2000

3. Click on the button **Change Settings...**. The dialogue shown in figure 4.16 will appear.

4. You can now select two independent certificates for signature and encryption using the **Choose...** buttons. **Be careful to select a certificate which contains the e-mail address suitable for your e-mail account!** You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 4.14.

5. You can select the session key algorithm which will be used for bulk encryption and decryption as well as the hashing algorithm for digital signatures. For strongest security, **3DES** or **RC2 128-bit** is recommended as encryption algorithm and **SHA1** as hashing algorithm.

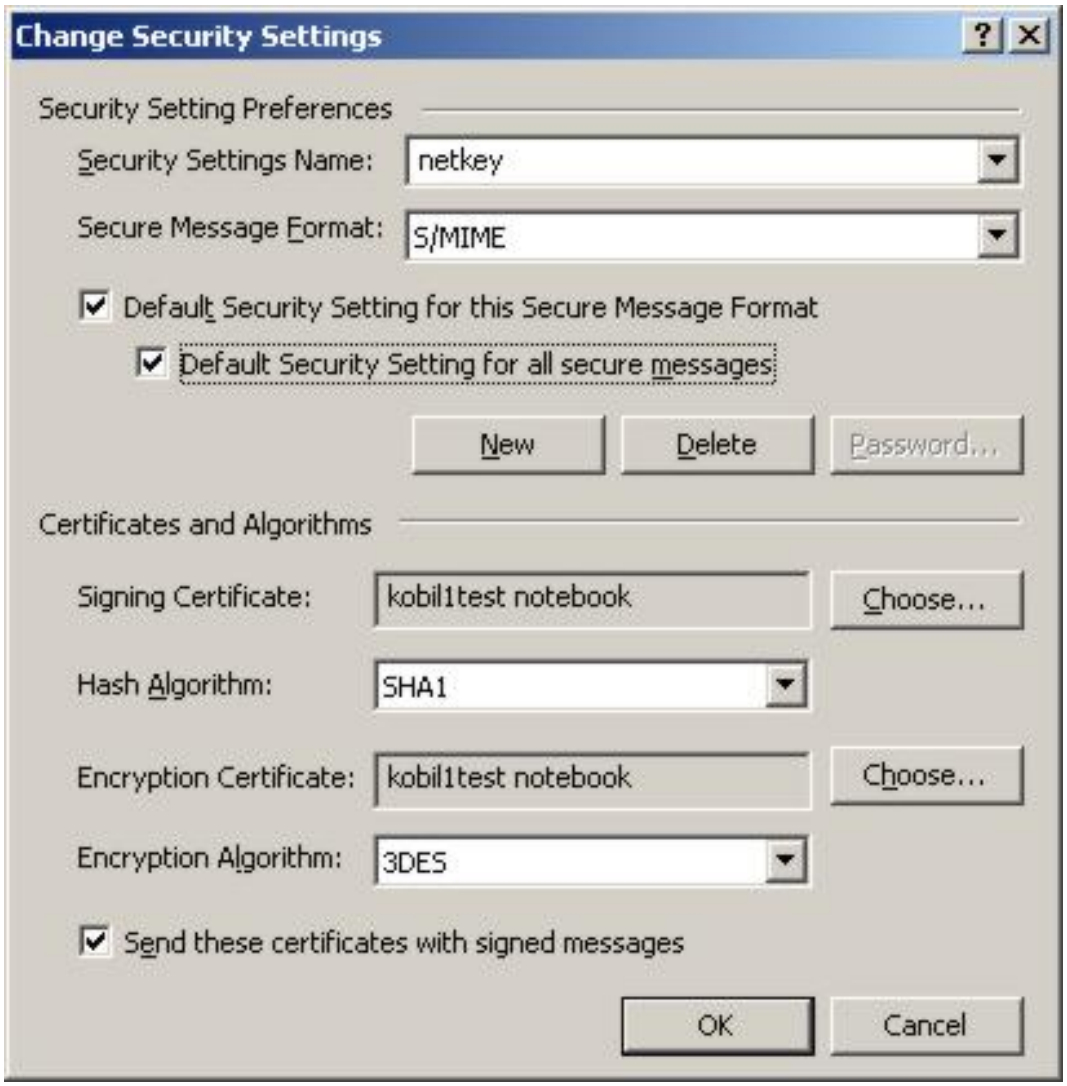

Figure 4.16: Outlook 98 / 2000 certificate selection

4.3.2 Sending secure E-mail

You can configure your default settings to sign and encrypt all outgoing messages (Click **Tools** > **Options** > **Security** and place checkmarks). If you do not define a default behaviour for signing and encryption, you can use **Sign** and **Encrypt** buttons of the new mail window. In Outlook 98/2000 these buttons do exist, but are hidden by default. You can make them appear by configuring your menu bar.

To send a signed e-mail, you need a certificate associated with your account. You can choose a signing certificate as default. You should present your card and the PIN to sign the message. Your e-mail will be signed as soon as you click on the **Send** button.

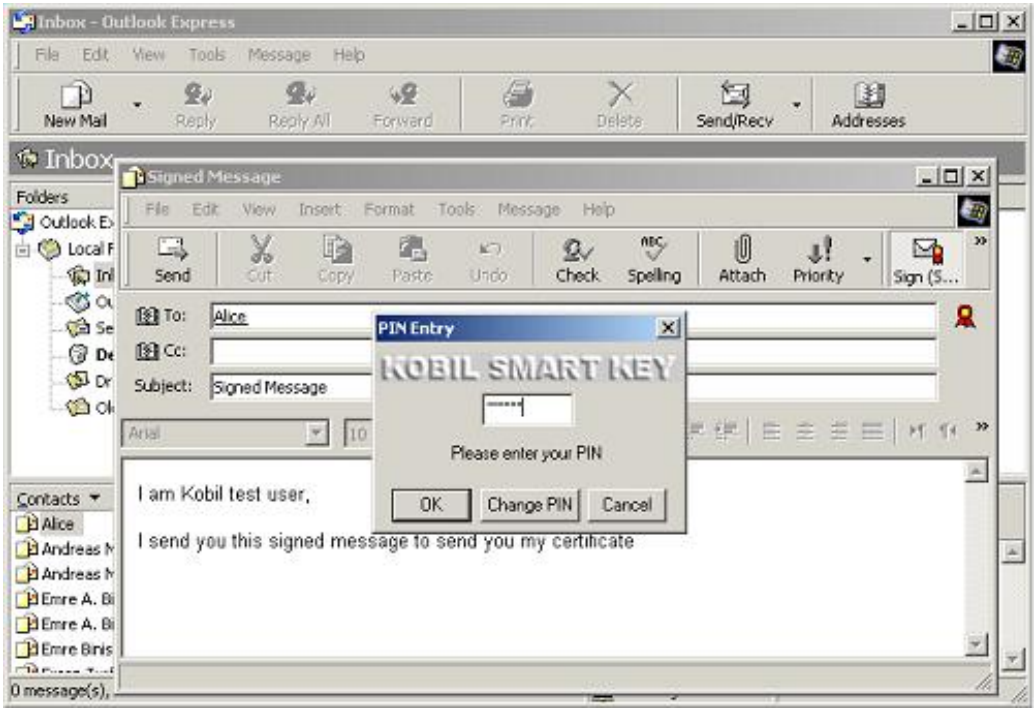

Figure 4.17: Signing an e-mail in Outlook Express

To send someone an encrypted message, you must have the recipient's certificate (see section 4.1.5). You can also sign the encrypted message.

4.3.3 Receiving secure E-mail

When you receive a signed message, your browser makes the necessary checks to verify if the sender's certificate and the signature of the message are valid. If someone has your certificate, he can send you encrypted messages. You are asked to insert your card and enter the card's PIN to decrypt the message.

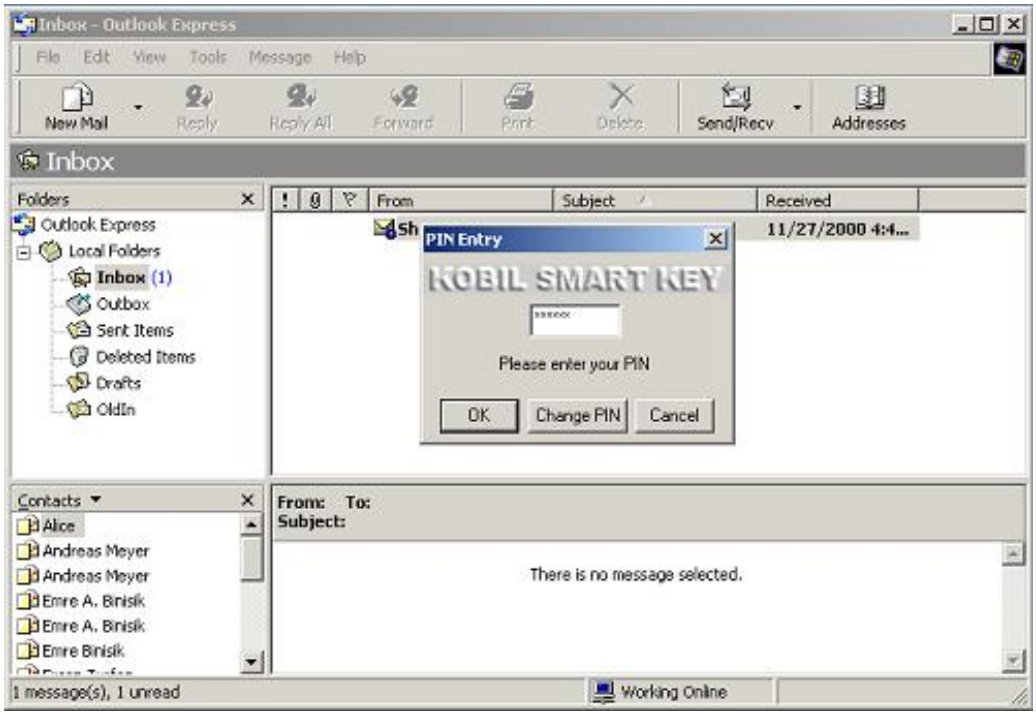

Figure 4.18: Receiving an encrypted E-mail in Outlook Express

Outlook Express shows encrypted messages with a blue sign and signed messages with a red sign. After a message signature is verified and the message is decrypted, you should click the **Continue** button (at the bottom of the e-mail) to see the mail content.

4.4 File Security

If you have choosen to install the file security option during setup, KOBIL Smart Key gives you the possibility to protect your files using your smart card. The following operations are possible:

- **Encryption:** Your files are encrypted with a certificate, so that it can only be decrypted using the corresponding private key on your smart card. Only the person owning both the right smart card and the card's PIN can access the file contents. You can encrypt **files and directories**.
- **Digital Signature:** By means of a digital signature, your data can be protected against unauthorized modification. Furthermore, the data can be assigned to the author. You can sign **files and directories**.
- **Encryption and Signature:** The advantages of encryption and signature are being combined.
- **Secure Erase:** Files and directories are securely erased (deleted) by multiple overwriting.

4.4.1 Additional Decryption Keys

The cryptograhpic mechanisms used in KOBIL Smart Key are so strong that nobody can recover the encrypted text without knowledge of the corresponding private key. Your private key is well-protected on your smart card. But it can of course happen that you lose your smart card or it is stolen. As the smart cards are PIN-protected, nobody can gain unauthorized access to your data.

To make those data accessible for yourself in such a case, KOBIL Smart Key optionally supports so-called *Additional Decryption Keys, ADK*. Using Additional Decryption Keys, every file and every directory you encrypt with your certificate is also encrypted with another configurable certificate that we call *Additional Decryption Certifikate*.

Each Additional Decryption Certificate of course also has a corresponding private key. This private key needs not to be located on a smart card. Depending on your security policy, the Additional Decryption private key is kept in a secure place like a bank tresor. It is not needed during normal operation.

In case where a file cannot be decrypted anymore because the corresponding private key is temporarily or forever unaccessible, it can still be decrypted using the Additional Decryption private key. To do so, the file must be present on a machine where KOBIL Smart Key is installed and where the Additional Decryption private key is registered – either as a software certificate or as another smart card.

Attention! Additional Decryption Keys are not used for e-mail encryption!

Additional Decryption Keys are configured by the CardManagement Tool as described in section 4.5.

4.4.2 File Encryption

If you want to encrypt a file, proceed as follows:

1. Right-click on the file you want to encrypt. The context menu shown in figure 4.19 appears.
2. Choose

KOBIL Smart Key > Encrypt

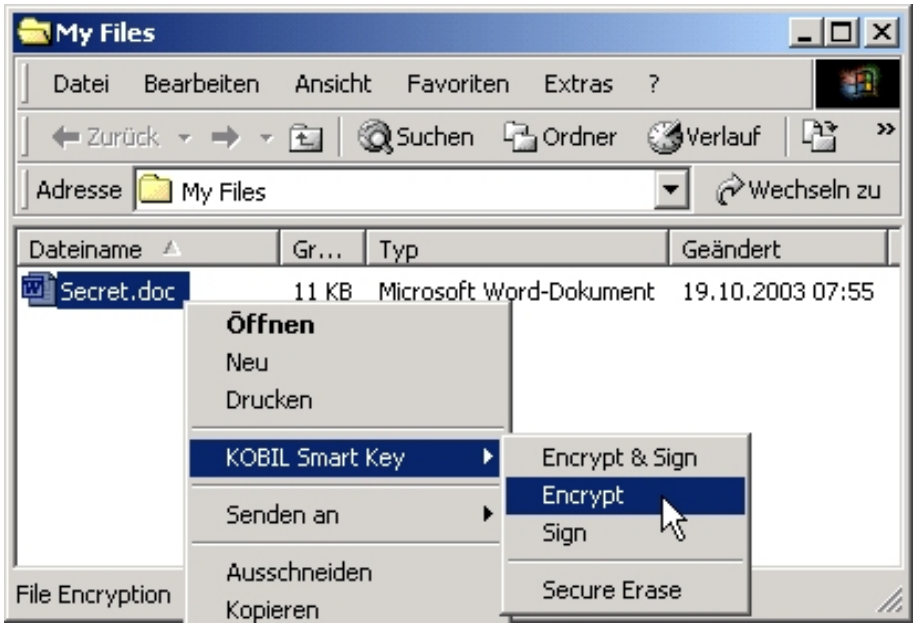

Figure 4.19: Context menu for file/directory encryption

3. The dialogue shown in figure 4.20 appears. The following options are possible:

   - **Encryption Certificate:** This is the default encryption certificate configured in CardManagement Tool (see section 4.5.5). If you want to use any other encryption certificate, click on **Choose**.
   - **Additional Decryption Key (ADK):** If there is an ADK configured in CardManagement Tool (see section 4.5), the corresponding certificate is shown here. Please verify. If you don't want ADK to be used, activate the checkbox **Don't use ADK**.
   - **Erase original file(s):** This checkbox decides if the original files should be erased after encryption. The default setting of this checkbox can be configured in CardManagment Tool (see section 4.5.5)
     Attention! If this checkbox is active and you are about to encrypt to a foreign certificate, you will not be able to recover those files!

   If all options are correctly set, click on **proceed** to start the encryption process.

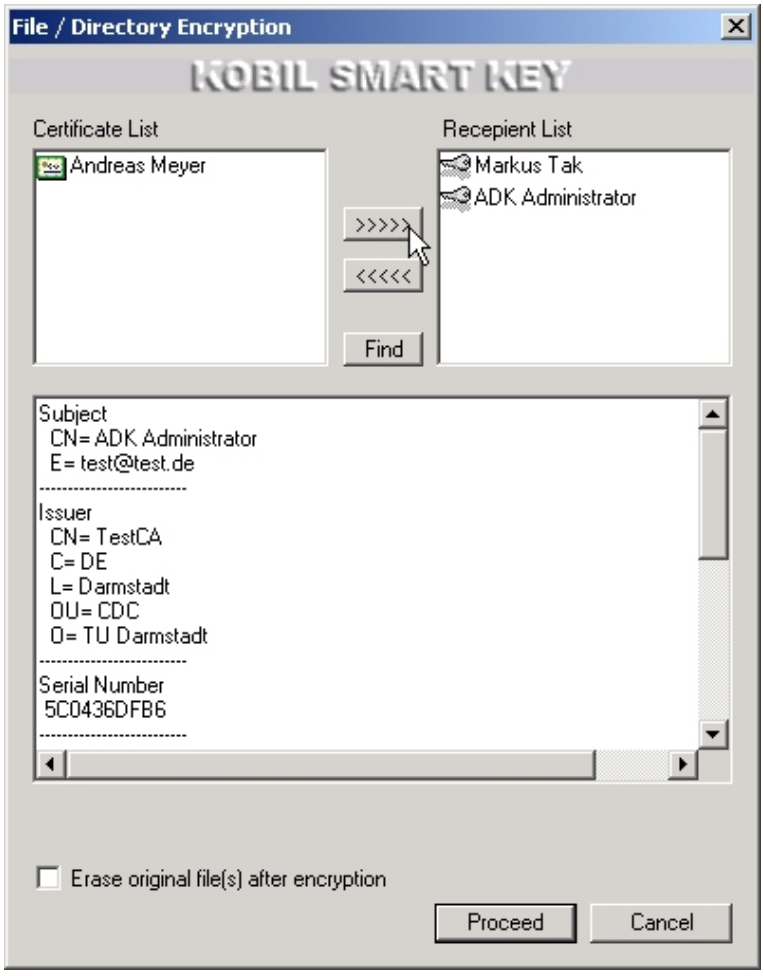

Figure 4.20: File/directory encryption options

4. Now the file(s) are encrypted and stored with the ending **.kse** as shown in figure 4.21.

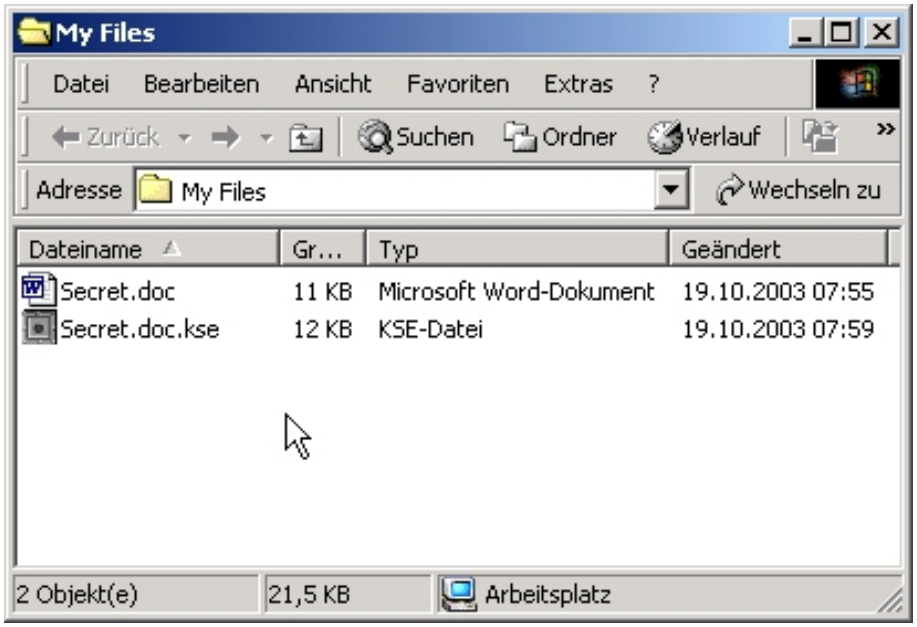
My Files
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Ordner Verlauf
Adresse My Files
Wechseln zu
Dateiname Gr... Typ Geändert
Secret.doc 11 KB Microsoft Word-Dokument 19.10.2003 07:55
Secret.doc.kse 12 KB KSE-Datei 19.10.2003 07:59
2 Objekt(e) 21,5 KB Arbeitsplatz

Figure 4.21: An encrypted file

Encrypted files are stored in PKCS#7 format which enabled interoperability between different applications.

Attention! Never encrypt files necessary for your operating system to start! You may destroy your system configuration!

4.4.3 File Decryption

You can recognize encrypted files by the ending **.kse**.

1. Right-click on the file you want to decrypt. The context menu shown in figure 4.22 is shown.
2. Choose

   KOBIL Smart Key > Decrypt

3. Insert your smart card and enter your PIN.
4. The file is now decrypted and stored without the ending **.kse**.
5. If the encrypted file is deleted after decryption, depends on the configuration in CardManagement Tool (see sections 4.5.5).

KOBIL Smart Key also decrypts files that were not encrypted using KOBIL Smart Key if they are in PKCS#7 format and you have the corresponding private key, of course.

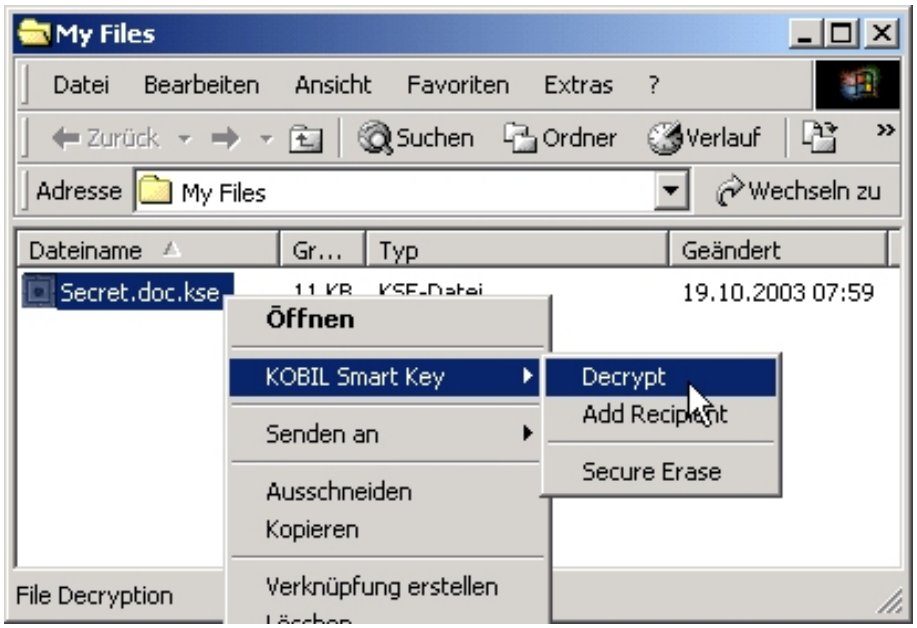

Figure 4.22: Context menu for file/directory decryption

4.4.4 Directory Encryption

Directory encryption works just like file encryption. If you encrypt a whole directory, all files inside this directory are encrypted seperately in one step.

Just follow the steps of section 4.4.2, where file encryption is described. Right-click the directory you want to encrypt instead of a file.

Every file inside that directory is encrypted in PKCS#7 format and stored with the ending **.kse**.

Attention! Never encrypt directories necessary for your operating system to start! You may destroy your system configuration!

4.4.5 Directory Decryption

Directory decryption works just like file decryption. If you decrypt a whole directory, all files inside this directory with the ending **.kse** are seperately decrypted in one step.

Just follow the steps of section 4.4.3, where file decryption is described. Right-click the directory you want to decrypt instead of a file.

Every file inside that directory with the ending **.kse** is decrypted. The ending **.kse** is removed and the file is stored in clear text.

4.4.6 File Signature

If you want to digitally sign a file, proceed as follows:

1. Right-click on the file you want to sign. The context menu shown in figure 4.23 is shown.

Figure 4.23: Context menu for file signature

2. Choose

KOBIL Smart Key > Sign

3. The dialogue shown in figure 4.24 appears. The following options are available:

   - **Signature Certificate:** This is the default signature certificate configured in CardManagement Tool (see section 4.5.5). If you want to use any other signature certificate, click on **Choose**.
   - **Erase original file(s):** This checkbox decides if the original files should be erased after signature. The default setting of this checkbox can be configured in CardManagment Tool (see section 4.5.5)

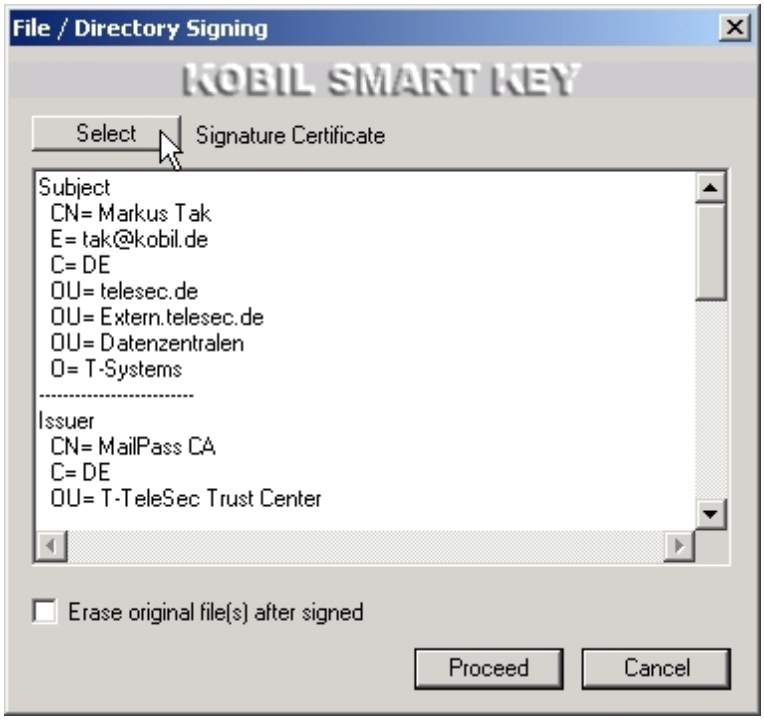

Figure 4.24: File/directory signature options

If all options are correct, click on **proceed** to start the signature process.

4. Insert your smart card and enter your PIN.
5. The file is now signed and stored with the ending **.kss** as shown in figure 4.25.

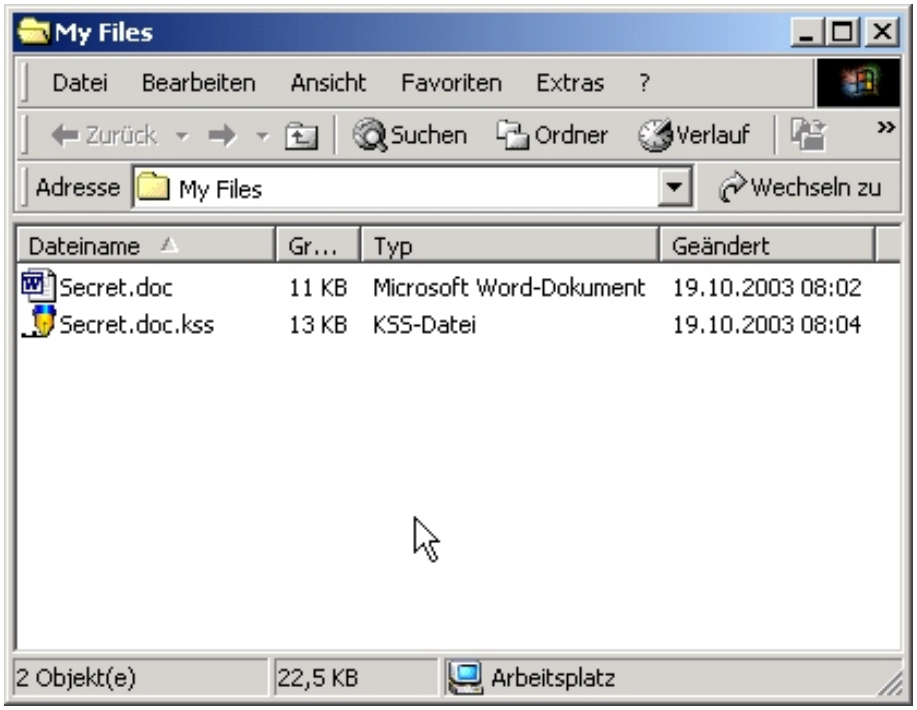

Figure 4.25: A signed file

Signed files are stored in PKCS#7 format which enabled interoperability between different applications.

4.4.7 File Signature Verification

To verify a file's digital signature, proceed as follows:

1. Right-click on the file with the ending **.kss** you want to verify. The context menu shown in figure 4.26 appears.

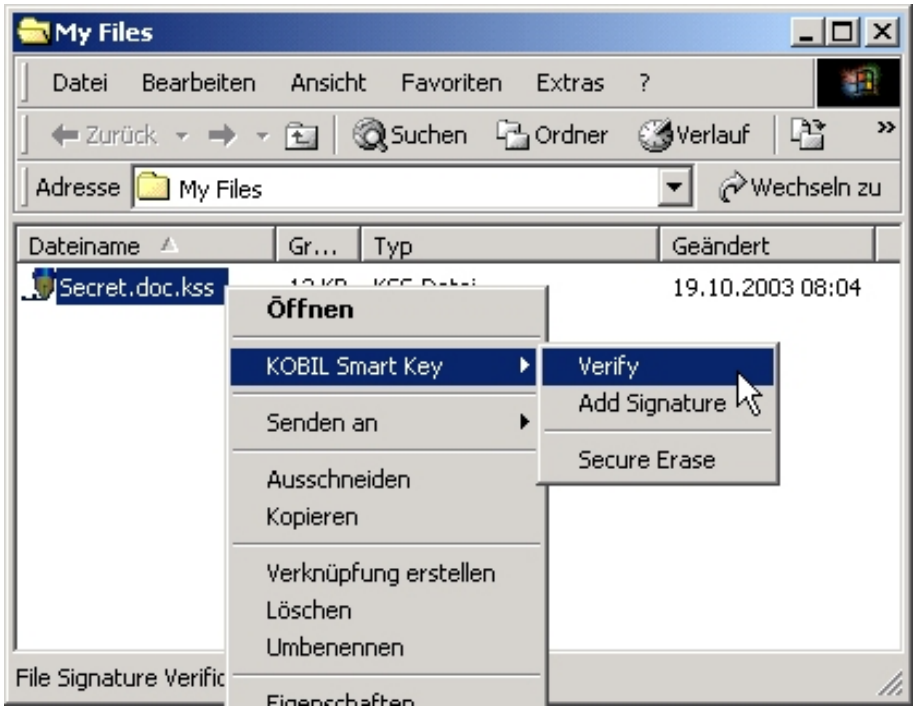

Figure 4.26: Context menu for file/directory signature verification

2. Choose

KOBIL Smart Key > Verify Signature

3. The status dialogue as shown in figure 4.27 appears. In the choice box, you can see the verification status for each file. Click on a file name to see the corresponding signature certificate below.

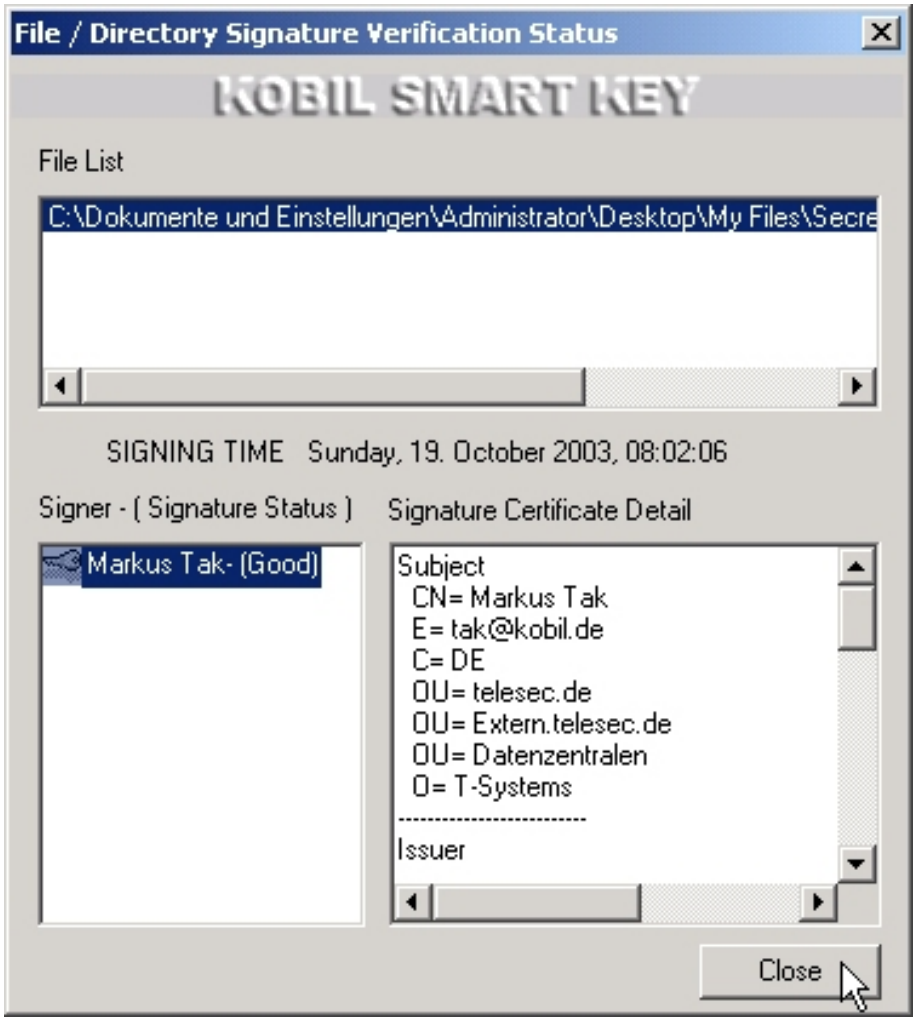

Figure 4.27: Signature Verification Status

4. All verified files are stored without the ending **.kss** in a new file. If the signature file (with the ending **.kss**) is deleted or not, depends on the configuration in CardManagement Tool as described in section 4.5.5.

4.4.8 Directory Signature

Directory signature works just like file signature. If you sign a whole directory, all files inside this directory will be seperately signed in one step.

Just follow the steps of section 4.4.6, where file signature is described. Right-click the directory you want to sign instead of a file.

Every file inside that directory will be signed in PKCS#7 format and stored with the ending **.kss**.

4.4.9 Directory Signature Verification

Directory signature verification works just like file signature verification. If you verify the signature over a whole directory, all files inside this directory will be verified in one step. The verification result will be displayed in one dialogue at the end.

Just follow the steps of section 4.4.7, where file signature verification is described. Right-click the directory you want to verify instead of a file.

Every file inside that directory will be verified and stored without the ending **.kss** in a new file.

4.4.10 Signature and Encryption of Files and Directories

If you want to encrypt and sign a file or a directory in one step, proceed as follows:

1. Right-click on the file or directory you want to encrypt and sign. The context menu shown in figure 4.28 appears.
2. Choose

   KOBIL Smart Key > Encrypt & Sign

Figure 4.28: Context mennu for file/directory signature and encryption

3. The dialogue shown in figure 4.29 appears. The following options are possible:

   - **Signature Certificate:** This is the default signature certificate configured in CardManagement Tool (see section 4.5.5). If you want to use any other signature certificate, click on **Choose**.

- **Encryption Certificate:** This is the default encryption certificate configured in CardManagement Tool (see section 4.5.5). If you want to use any other encryption certificate, click on **Choose**.
- **Additional Decryption Key (ADK):** If there is an ADK configured in CardManagement Tool (see section 4.5), the corresponding certificate is shown here. Please verify. If you don't want ADK to be used, activate the checkbox **Don't use ADK**.
- **Erase original file(s):** This checkbox decides if the original files should be erased after encryption/signature. The default setting of this checkbox can be configured in CardManagment Tool (see section 4.5.5)
  Attention! If this checkbox is active and you are about to encrypt to a foreign certificate, you will not be able to recover those files!

If all options are correctly set, click on **proceed** to start the encryption/signing process.

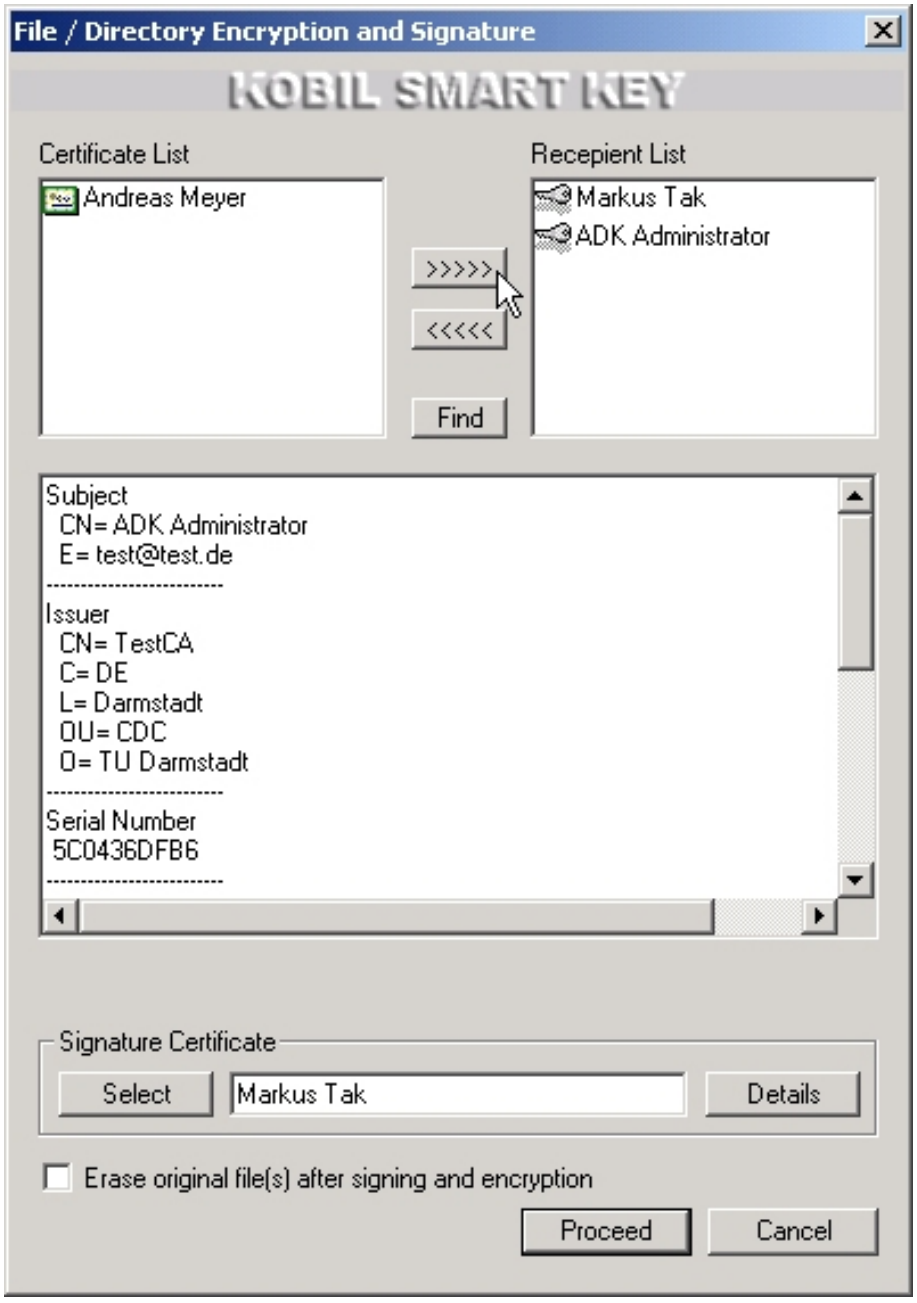

Figure 4.29: File/directory encryption and signature options

4. Insert your smart card and enter your PIN.

5. The file (e.g. all files inside the chosen directory) are now encrypted and signed and stored with the ending **.ksk** as shown in figure 4.30. If a directory is processed, the ending **.ksk** is also appended to the directory name.

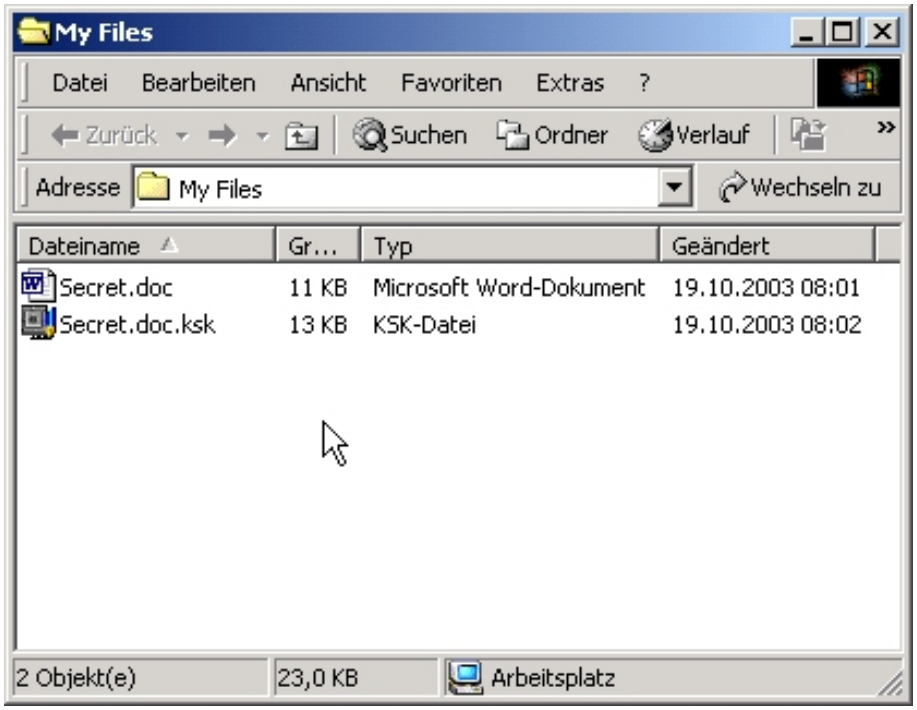
My Files
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Ordner Verlauf
Adresse My Files
Wechseln zu
Dateiname Gr... Typ Geändert
Secret.doc 11 KB Microsoft Word-Dokument 19.10.2003 08:01
Secret.doc.ksk 13 KB KSK-Datei 19.10.2003 08:02
2 Objekt(e) 23,0 KB Arbeitsplatz

Figure 4.30: A signed and encrypted file

Encrypted and signed files are stored in PKCS#7 format which enabled interoperability between different applications.

Attention! Never encrypt files necessary for your operating system to start! You may destroy your system configuration!

4.4.11 Signature Verification and Decryption of Files and Directories

Signed and encrypted files and directories have always attached the ending **.ksk** in their name. If you want to decrypt and verify the signature of a file or a directory in one step, proceed as follows:

1. Right-click on the file or directory you want to decrypt and verify. The context menu shown in figure 4.31 appears.
2. Choose

KOBIL Smart Key > Decrypt & Veriy

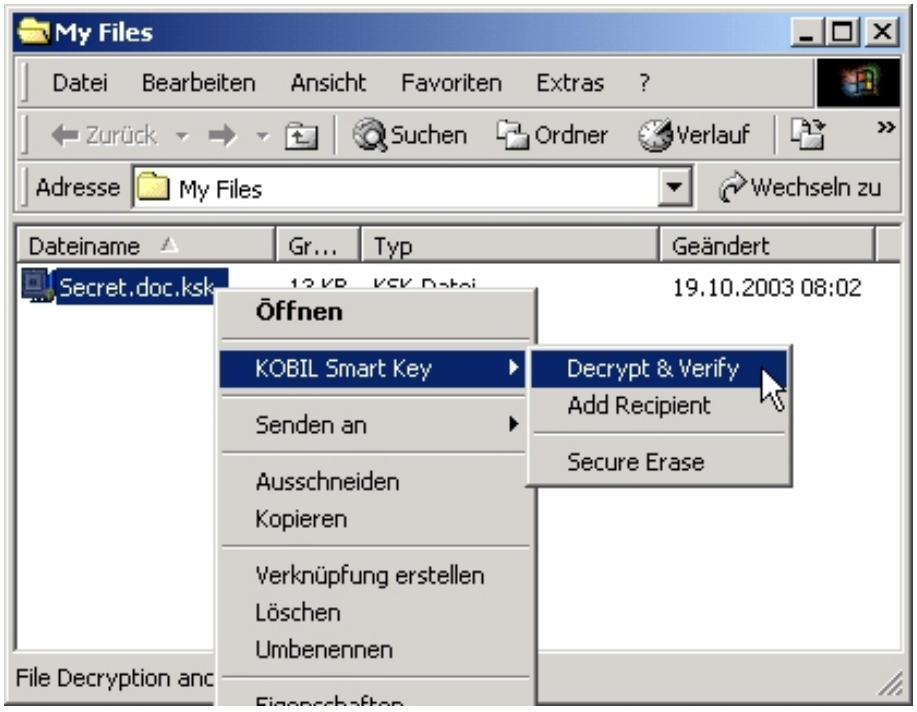

Figure 4.31: Context mennu for file/directory signature verification and decryption

3. Insert your smart card and enter your PIN.

4. The file (e.g. all files inside the chosen directory) are now decrypted and verified and stored without the ending **.ksk**. The ending **.ksk** is also removed from the directory name. The signature verification result is shown as in figure 4.27.

4.5 The CardManagement Tool

CardManagement Tool is a utility that contains some important functions required to manage your smart cards and the certificates on them. During normal usage, you won't need CardManagement Tool, it's only required for configuring KOBIL Smart Key. The following functions are available:

1. **Register Certificates in the Windows Certificate Manager**
   If you want to use your certificates with the Internet Explorer or Outlook, they have to be registered in the windows certificate manager. This happens automatically for certificates that are enrolled using the Internet Explorer on that machine as described in section 4.1.2.
   Certificates, that
   - **have not been enrolled on that machine** or
   - **have been enrolled using another application (e.g. Netscape)**

   and should be used with Internet Explorer or Outlook on your machine, must be registered manually using the CardManagement Tool.
2. **Deletion of Certificates from your smart card**
   If you don't need a certificate anymore, you can delete it from your smart card using CardManagement Tool.
3. **Import Certificates to your smart card**
   Existing software certificates and corresponding private keys can be loaded on your smart card. This can be necessary during a migration from software- based certificates to smart cards, but note that this is somewhat risky, since the private keys have not been stored inside the security environment of your smart card without interruption!
4. **Changing the smart card's PIN**
5. **Default Settings for File Security**
   Default setting for the file security operations described in section 4.4 can be done using CardManagement Tool to simplify the daily use. Additional Decryption Keys as described in section 4.4.1 can be set-up and managed using CardManagement Tool.

The CardManagement Tool runs permanently in the Windows Tray bar on the right botton of your desktop, next to the clock.

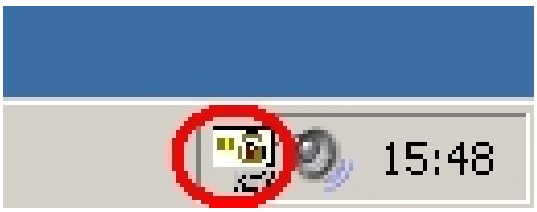

Figure 4.32: CardManagement Tool in the Tray bar

Double-click on the CardManagement Tool icon to launch its user interface. Figures 4.33 to 4.35 show the user interface of CardManagement Tool:

- **Certificates:** Here, you see all certificates supported by the current KOBIL Smart Key configuration.
- **Card:** Allows to configure global card functions
- **File Security:** Configuration of file security default settings.

4.5.1 Registering certificates for the Windows Certificate Manager

Choose the drawer **Card** in CardManagement Tool and click on **Read Card**. Insert your smart card and enter your PIN. Now, all certificates present on your smart card are read-out. After that, you can choose them in the drawer **Certificates** seperately and click on **Register** to register them or click on **Details** to take a look at them. The **Unregister** button unregisters the selected certificate, but does not delete it. You can re-register it anytime you want.

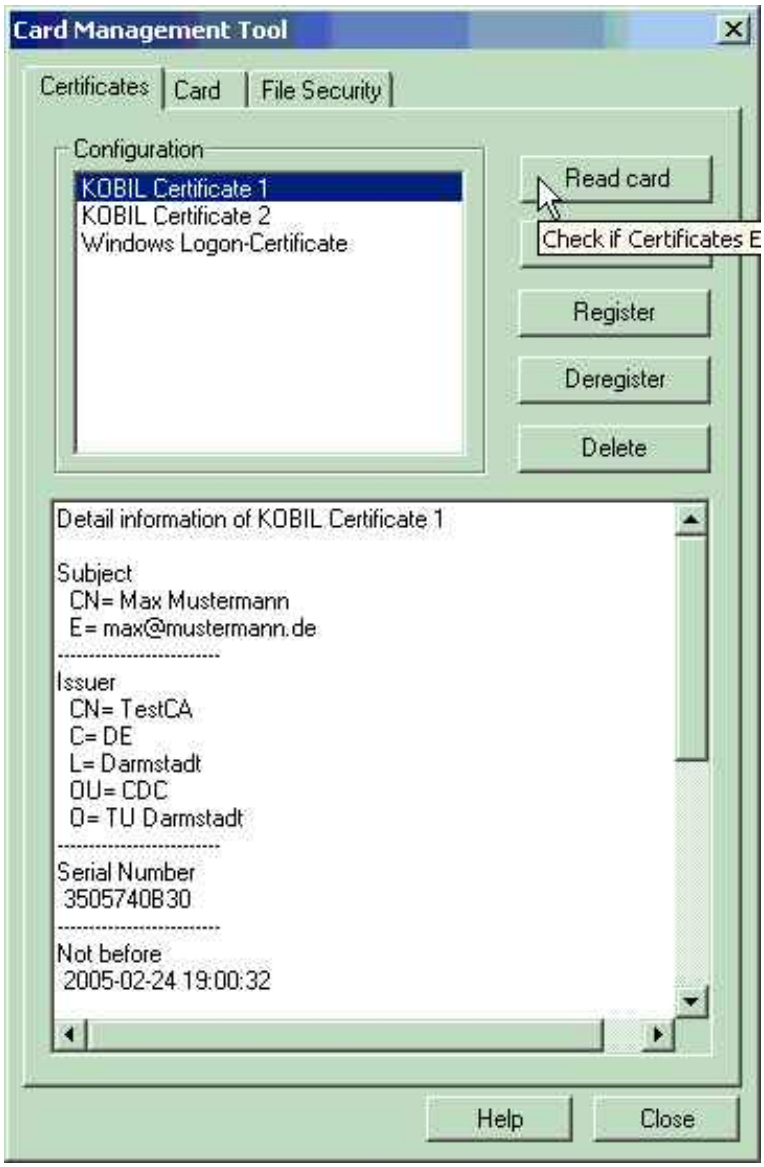

Figure 4.33: CardManagement Tool - Certifikates

A more simple way to register all certificates on your TCOS smarcard is to run once the program

Start > Programs > KOBIL Systems > KOBIL Smart Key > Register Certificates

You will be asked to insert your smart card. All certificates on your smart card will be registered automatically.

4.5.2 Deletion of Certificates from your smart card

Be very careful with certificate deletion, since any e-mail, file or directory encrypted with that certificate cannot recovered after!

Choose the certificate to delete in the drawer **Certificates** and click on **Delete**.

Depending on your configuration, certificate deletion may be disabled for security reasons.

4.5.3 Importing Certificates onto your smart card

KOBIL Smart Key allows you to load software-based certificates (e.g. certificates and private keys stored in PKCS#12 files) from the windows certificate manager onto your smart card if they are marked as **exportable**. To do so, click on the **Import Cert** button in the **Card** drawer.

If you have your software-certificate only as a PKCS#12 file (e.g. a file whose name ends with **.p12**), you'll have to import it into the windows certificate manager first by double-clicking it. Follow the instructions of the windows certificate manager during the import and mark the private key as **exportable**.

We strongly recommend to delete the software certificate from the windows certificate manager after successfully importing it onto your smart card for security reasons!

Depending on your configuration, this function may be disabled for security reasons.

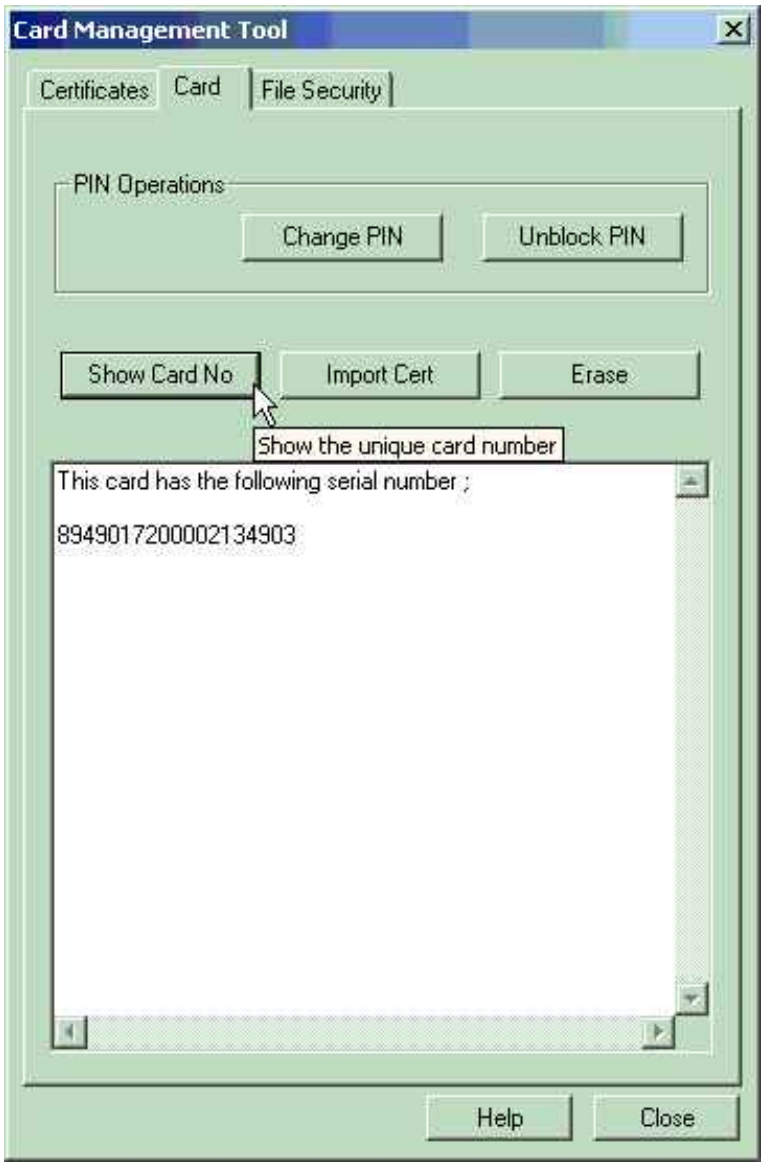

Figure 4.34: CardManagement Tool - Card

4.5.4 Change / Unblock tge PIN of your Smart Card

If you want to change the PIN of your smart card, click on the **Change PIN** button in the **Card** drawer. You will have to enter your old PIN and then twice your new PIN. Depending on your chipcard terminal, you must enter the PIN either via your computer's keyboard or via the terminal's keypad (*Secure PIN-entry*).

Depending upon your configuration, you have the possibility to unblock the PIN using a PUK as you may know from your mobile phone SIM card. This may become necessary if your PIN is blocked after three wrong entries. You can do this by clicking the **Unblock PIN** button in the **Card** drawer of CardManagement Tool. If you don't know the card's PUK, please contact your Administrator.

4.5.5 Default Settings for File Security

Choose the drawer **File Security** in Cardmanagement Tool.

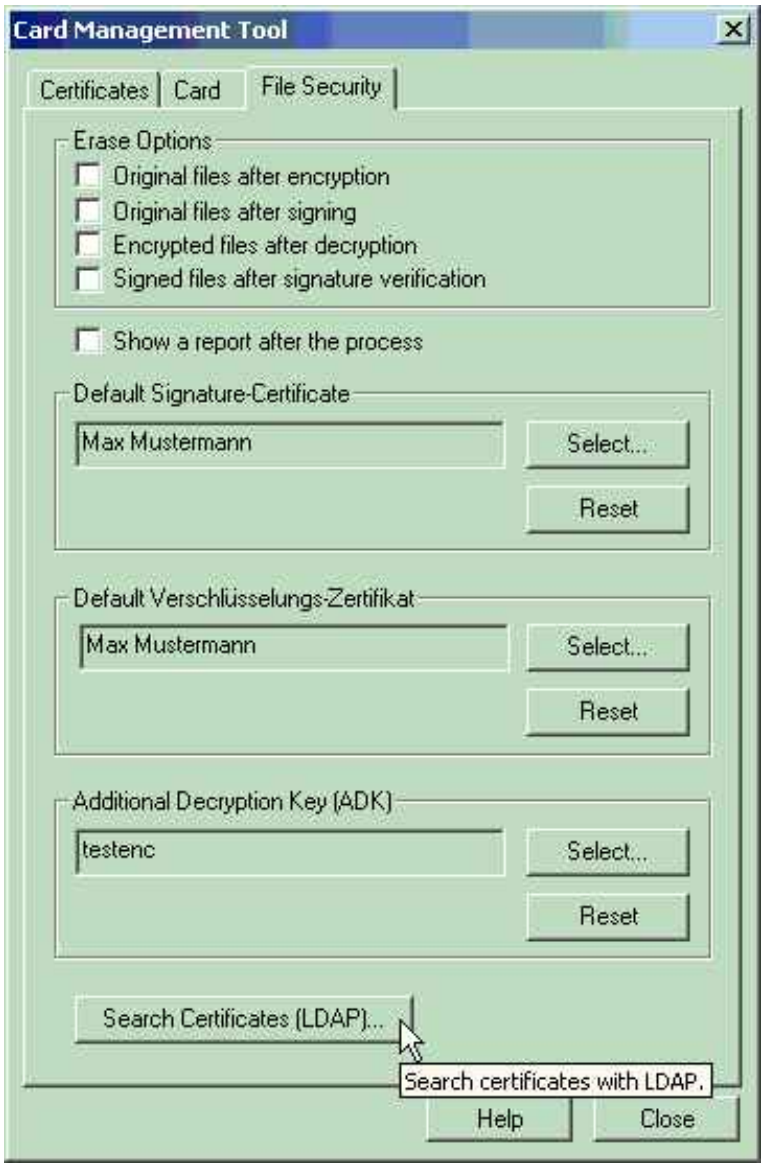

Figure 4.35: CardManagement Tool - File Security

Erase Options

- If the checkbox **Original files after encryption** is active, each original file is deleted automatically after encryption. You can change this behaviour also per encryption process (see sections 4.4.2, 4.4.4 and 4.4.10).
- If the checkbox **Original files after signing** is active, each original file is deleted automatically after signature. You can change this behaviour also per signature process (see sections 4.4.6 and 4.4.8).

- If the checkbox **Encrypted files after decryption** is active, each encrypted file is deleted automatically after decryption.
  Note that this option cannot be changed per decryption process!
- If the checkbox **Signed files after signature verification** is active, each signed file is deleted automatically after signature verification.
  Note that this option cannot be changed per signature verification process!

Show Report after Process

If you enable this option, you will see a report about how many files have been processed in case you selected multiple files or even complete folders to encrypt, decrypt, sign, verify or secure erase.

Default Signature Certificate

Under *Default Signature-Certifikate*, click *Select*. You can select the default signature certificate from the list of all valid signature certificates (see section 4.4.6). The button *Reset* disables the default signature certificate.

Important: this setting does NOT have any impact on *qualified signatues*

Default Encryption Certificate

Under *Default Encryption-Certifikate* click on *Select*. You can select the default encryption certificate from the list of all valid encryption certificates (see section 4.4.2). The button *Reset* disables the default encryption certificate.

Additional Decryption Key

Under *Additional Decryption Key* click on *Select*. You can select the Additional Decryption Key from the list of all valid encryption certificates. The button *Reset* disables the Additional Decryption Key.

Please read section 4.4.1 carefully before changing Additional Decryption Key configuration!

An ADK certificate has only impact on file and directory encryption, NOT on e-mail encryption!

Search Certificates

Using this button, you open a search dialogue that allows you to look up other people's certificates stored in so-called *directory services* and store them in your local Windows certificate store. This is a very useful function if you often encrypt files to other people.

Directory services are managed by Outlook and Outlook Express. If you don't want to use one of the pre-configured directory services, you should configure your individual directory service first, as described in section 4.1.5

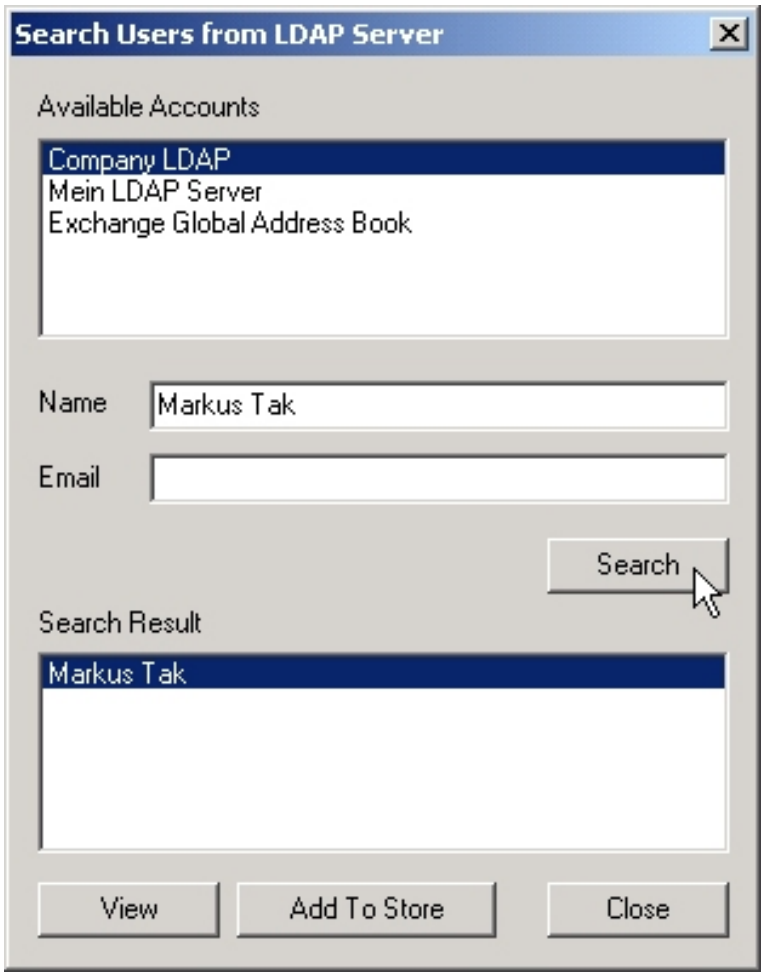

Figure 4.36: CardManagement Tool - Search Certificates

The dialogue shown in figure 4.36 shows all directory services configured in Outlook and Outlook Express. You can search for the person's name or email address. If one or more results have been found, you can show them and import them into the Windows certificate manager where they will be displayed in *Other People* as described in section 4.1.3.

Note:
If you want to search for user certificates in Active Directory, please configure a new directory service account for Active Directory first as described in section 4.1.5. As server name, please enter the domain controller's full DNS name. The search base must be written in the so-called "DC-notation". Example: if your domain is called "myDomain.myCompany.de", the DC notation will be "dc=myDomain, dc=myCompany, dc=de".

Chapter 5

Smart card Logon for Windows 2000/XP

In this section, you'll learn how Windows 2000 and Windows XP/ 2003 Server networks are secured by smart card logon using KOBIL Smart Key. The users will be able to log in with their smart cards into the network instead of static passwords.

Note: Smart Caard Logon is only available for Windows 2000 and XP domain member clients. Other Windows versions like Windows NT, as well as workgroup computers without domain membership are not supported. As domain controller, you can use Windows 2000 or a 2003 Server.

Note: To be able configure Windows for smart card logon, one must have deeper knowledge about Windows administration. In this manual, we can only show the steps concerning directly KOBIL Smart Key. Further configuration, e.g. policy settings, may be necessary to satisfy your particular security policy.

5.1 Prerequisites

Windows 2000 and XP make it possible to deploy strong authentication using smart cards by leveraging operating system features such as Kerberos, Active Directory, and the variety of administrative tools used to manage a public key infrastructure. To use the smart card logon feature, you can pursue the following steps or you can get more information from Windows 2000 / 2003 Server help.

1. **A PCSC driver for your KOBIL smart card terminal must be installed on every client machine! A CT-API driver will not work.** To find out if a PCSC driver is installed, open the device manager in the system configuration panel and take a look if a KOBIL smart card terminal appears there. If not, you'll have to install a PCSC driver first.
2. Install at least one Windows 2000 / 2003 Server in your network as a domain controller.
3. Install the following optional components on your server in the same order:
   (a) Domain Name Service (DNS)
   (b) Active Directory
   (c) Certification Authority
4. Logon into domain as Administrator.
5. If you want to issue smart cards from another computer, make sure that DNS is configured correctly and that this computer is member of the domain.

6. Get and install an Enrollment Agent Certificate (see section 5.2).
7. Define users in Active Directory.
8. Issue a smart card logon certificate for each user (see section 5.3).
9. Each Computer in your network that will be equipped with smart card logon, needs an installed KOBIL Smart Key software (each a seperate licence) and a KOBIL smart card reader.

5.2 Enrollment Agent Certificate

An administrator needs an Enrollment Agent Certificate to issue Smart Card Logon Certificates. Follow these steps to get an enrollment agent certificate. If you logon from a different computer than the server, make sure that this computer is correctly configured as a domain member.

1. Run the Certificate Authority from the start menu:
   Start > Programs > Administrative Tools > Certificate Authority
2. Right-click **Policy Settings** under the name of your CA and select
   New > Certificate to issue

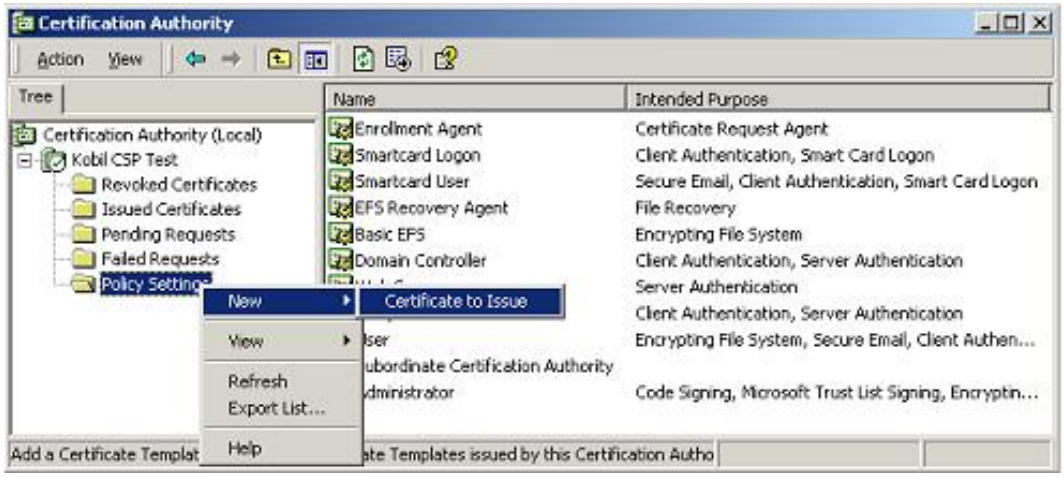

Figure 5.1: Certificate Authority

3. Add those Certificate Templates from the list: **Enrollment Agent**, **Smart Card Logon** and **Smart Card User**.

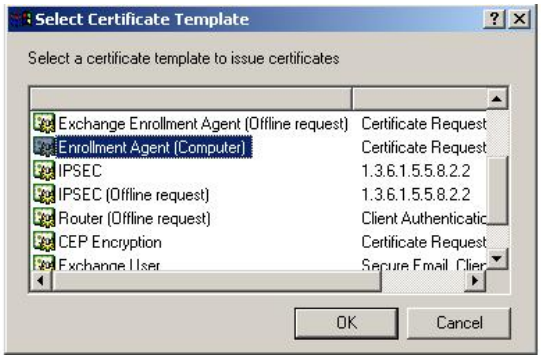

Figure 5.2: Certificate Templates

4. Close the Certification Authority console.
5. Run Microsoft Management Console (*mmc* from the command prompt).
6. Click **Console** > **Add/Remove Snap-in**

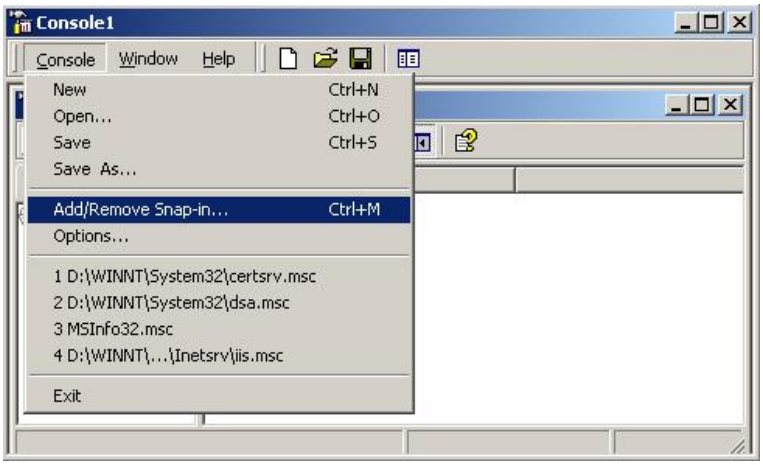

Figure 5.3: Add/Remove Snap-in in the MMC

7. Click **Add**, select **Certificates**, click **Add**, select **My User Accounts**, click **Finish** > **Close** > **Ok**

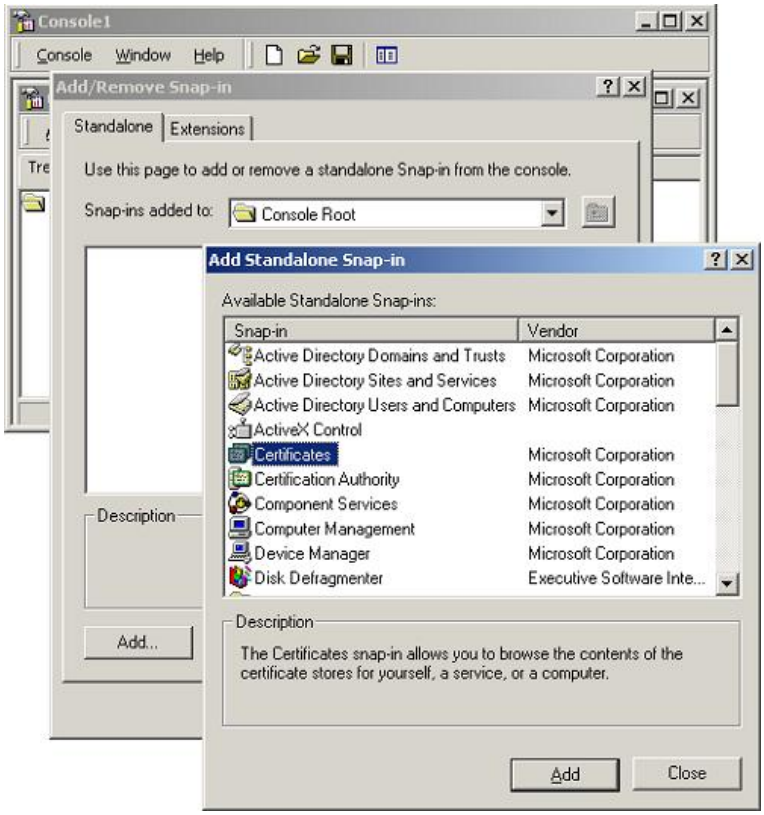
Console1
Console Window Help
Add/Remove Snap-in
Standalone Extensions
Use this page to add or remove a standalone Snap-in from the console.
Snap-ins added to: Console Root
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in Vendor
Active Directory Domains and Trusts Microsoft Corporation
Active Directory Sites and Services Microsoft Corporation
Active Directory Users and Computers Microsoft Corporation
ActiveX Control
Certificates Microsoft Corporation
Certification Authority Microsoft Corporation
Component Services Microsoft Corporation
Computer Management Microsoft Corporation
Device Manager Microsoft Corporation
Disk Defragmenter Executive Software Inte...
Description
Add...
Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
Add
Close

Figure 5.4: Adding Snap-in

8. Right click on **Personal** under **Certificates** and select **All Tasks** > **Request New Certificate...** from the menu. The Certificate Request Wizard will be started.

Figure 5.5: Request New Certificate

9. Click **Next**, select **Enrollment Agent** from certificate templates, click **Next**, write a **friendly name**, click **Next** > **Finish** > **Install**

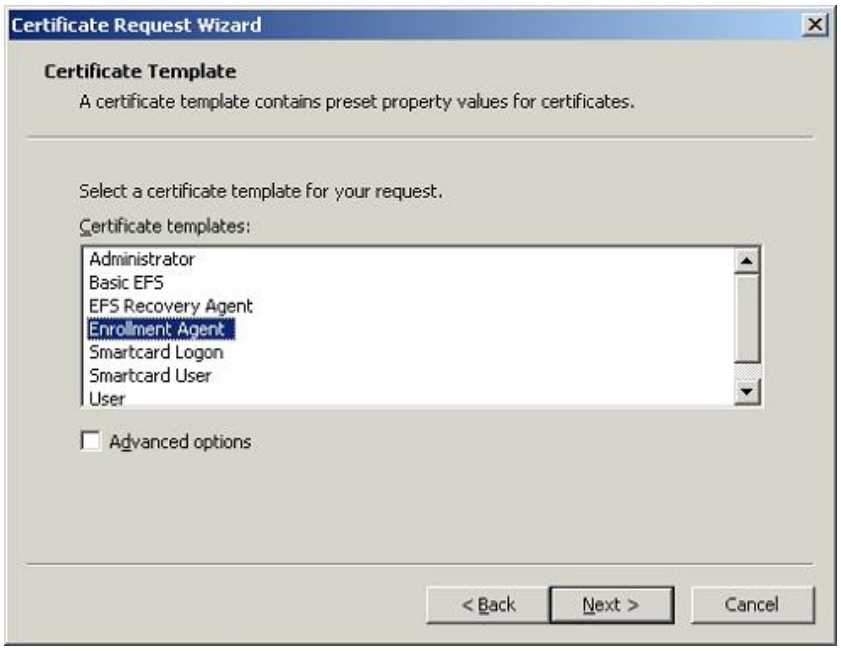

Figure 5.6: Certificate Request Wizard

5.3 Issuing Smart Card Logon Certificates

These steps have to be performed for each user who shall obtain a smart card for logon.

1. The Administrator who has the Enrollment Agent Certificate must logon into the CA web page by using Internet Explorer. The address is

   http://x.x.x.x/certsrv (x.x.x.x is the server's DNS address)

Figure 5.7: Password Dialog

2. Select **Request a certificate** and click **Next**

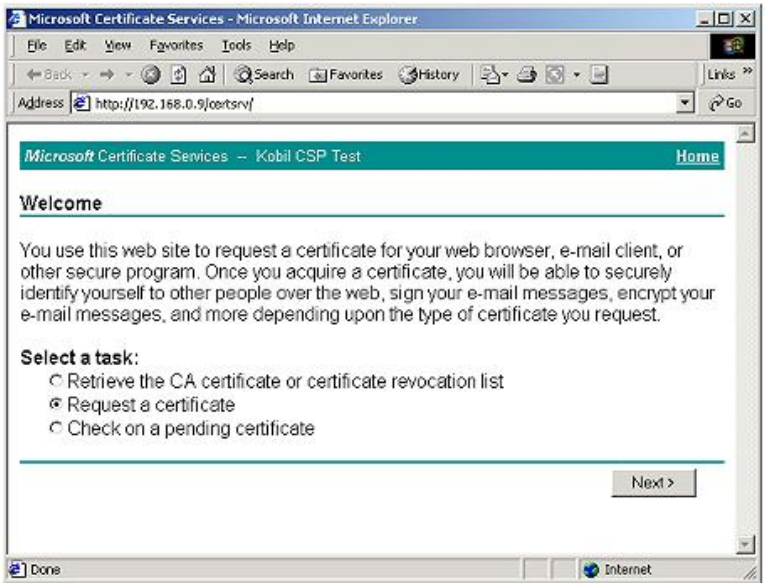
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
Address http://192.168.0.9/certsrv/
Go
Microsoft Certificate Services -- Kobil CSP Test
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
Done
Internet

Figure 5.8: Microsoft Certificate Service

3. Select **Advanced Request** and click **Next**

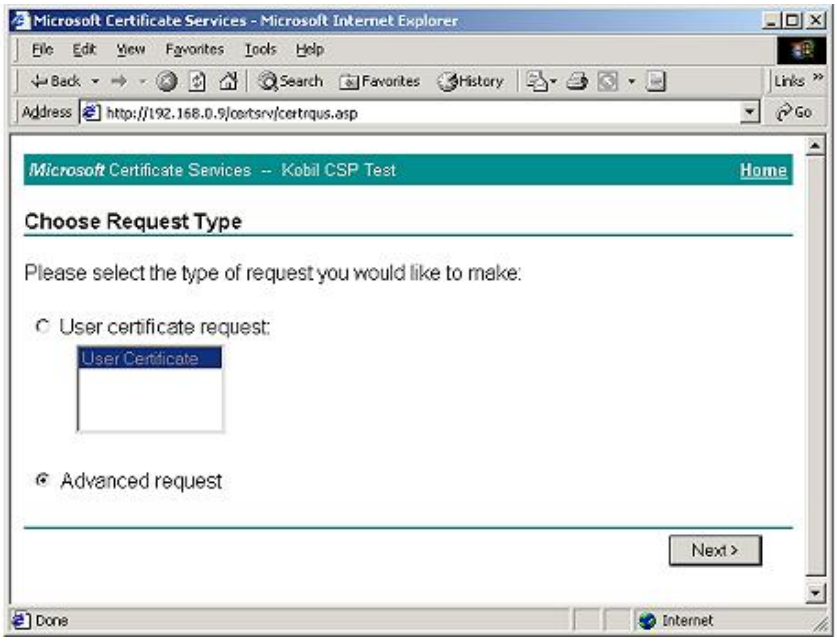

Figure 5.9: Choosing Request Type

4. Select **Request a certificate for a smart card** and click **Next**

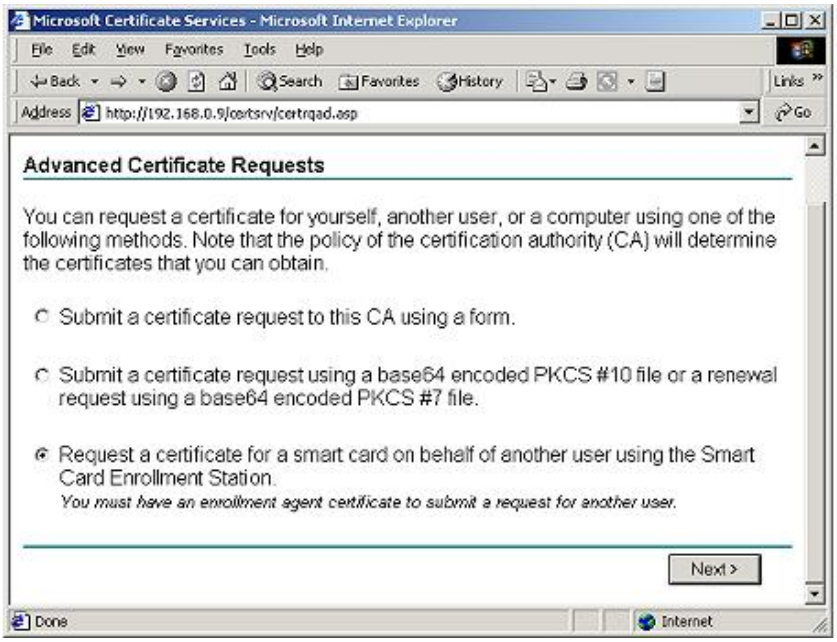

Figure 5.10: Advanced Certificate Request

5. Select the template **Smart Card Logon**, your CA as Certification Authority and **KOBIL Smart CSP v1.0** as CSP. Your enrollment agent certificate should be selected under **Administrator's Enrollment Agent Certificate**. Select the **user** to be enrolled from Active Directory. Insert an empty smart card and click **Enroll**. You will be prompted for the card's PIN. After enrollment is finished, you can view the logon certificate and continue the same process for another user with another card.

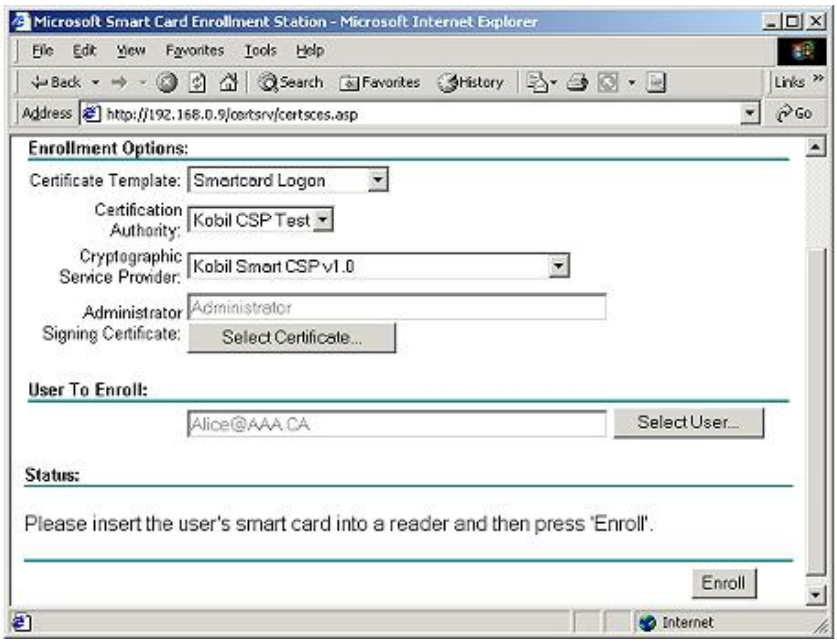

Figure 5.11: Enrollment Options

5.4 The Smart Card Logon Process

If Windows 2000 or XP detects a PC/SC compatible reader at start up, it gives the option to use a smart card for logon instead of a password.

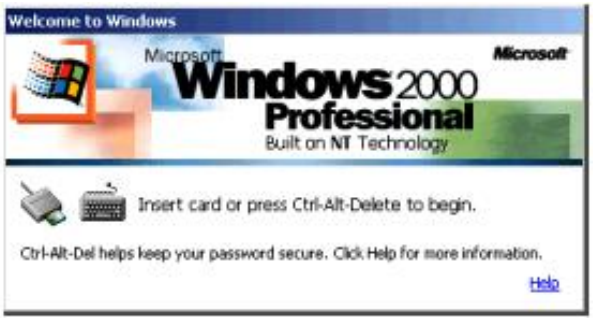

Figure 5.12: Windows 2000 Logon Dialog

Interactive Logon using a smart card begins with the user inserting a smart card into a smart card reader. After this, Windows will prompt for a Personal Identification Number (PIN) instead of a username, domain name and password. The card insertion event is equivalent to the familiar *Ctrl +Alt + Del* sequence used to initiate a password-based logon. However, the PIN the user provides to the logon dialog is used to authenticate only to the smart card and not to the domain itself. The logon certificate in the smart card is used to authenticate the user to the domain.

Figure 5.13: PIN Entry Dialog

If smart card logon fails with some error dialogues, please take a look at section A.2.

5.5 Important notes about Windows 2000 / XP Smartcard Logon

Logon procedure is aborted with the message that the smart card is not trusted:

Just after installing Windows 2000/2003 CA, it can take some time until the CA certificate and the certificat revocation list (CRL) have been published into Active Directory and to all client machines. Windows Group Policy interval defaults to 8 hours. This also happens if a new client machine has joined the domain. You can speed this time up by running **gpupdate /force** on a Windows 2003 Server. First, you should ensure that you can log on to the server locally (this requires to change the local security policy for domain controllers to allow users to log on interactively).

Lock Workstation when removing Smart Card:

This setting can be done on the domain controller for the whole domain. Click the following on your DC:

Start > Programs > Administrative Tools > Domain Security Policy

Choose in the **local policies** the **security options**. In the list you find the policy setting **smart card removal behaviour**. You can set this policy to **ignore**, **lock workstation** or **log off user**.

Please note that this setting is valid for all machines in the domain, but not for the domain controller itself.

Key Backup and AutoEnrollment

Windows 2003 CA has some interesting new features, two of them are key archival and certificate auto enrollment. Both of them are supported by KOBIL Smart Key, please take care about the corresponding settings in the certificate templates.

To recover archived keys, you need the **Key Recovery Tool krt.exe**, which is contained in the Windows 2003 Server Resource Kit that you can download at Microsoft's web pages.

Please note that Netkey 2000/E4 smart cards do not support key backup by default, since they have built-in keys that can not be read out and archived. But with some special configuration, you can define new keys on those cards which can be archived. To learn more about this, please contact your local KOBIL dealer or KOBIL directly.

5.6 Smart Card Logon for Terminal Server Environments

Using KOBIL Smart Key, you can also secure Terminal Services. Citrix Metaframe XP FR2 as well as Windows 2003 Server are able to forward PC/SC connections from the terminal client to the terminal server, so it is only necessary to install KOBIL Smart Key on the server and PC/SC drivers on the clients.

Further information can be found in the KOBIL Integration Guide *Integrating KOBIL Smart Key with Citrix Metaframe* which you can obtain from KOBIL.

KOBIL Smart Key also supports Microsofts Windows 2003 Terminal Server. In this case, it is important to have the most recent RDP Client (at least version 5.2) installed on your client machines. You can find this update for example on your Windows 2003 Server CD-ROM in the Tools directory. Once RDP is installed, you can select to map local smartcard readers to the terminal session, as shown in figure 5.14.

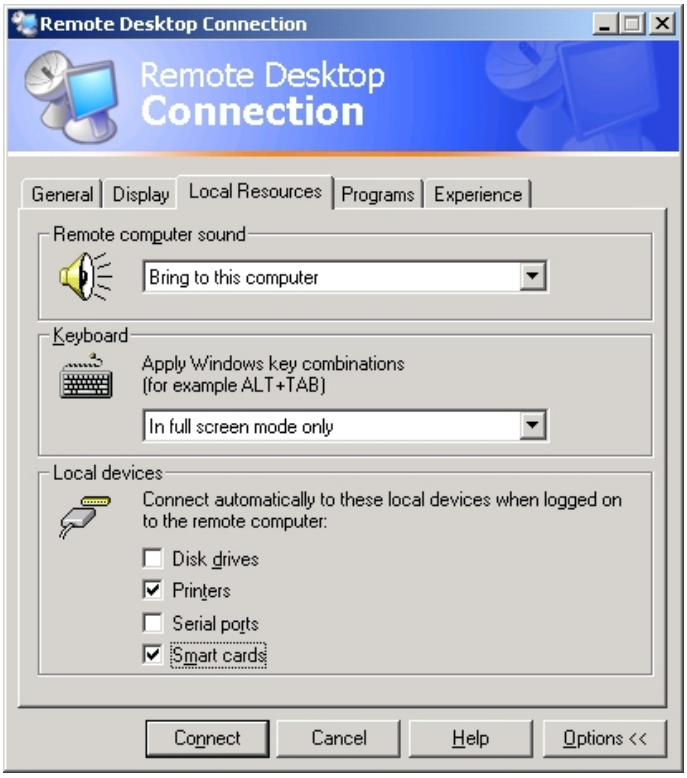

Figure 5.14: Remote Desktop Conntection (RDP) using Windows 2003 Server

Chapter 6

Using the KOBIL Smart Key PKCS#11 Module for Netscape

The KOBIL Smart Key PKCS#11 module was optimized for usage with Netscape Communicator, but you can use it also independently from Netscape.

6.1 Certificate Management with Netscape

Netscape has a build-in certificate manager that runs independenty from the windows certificate manager on windows platforms. In this section, you learn about the Netscape certificate manager.

6.1.1 Getting your Certificate

You must follow these steps if you do not have a certificate on your TCOS smart card yet. However, in some cases **you get a personalized TCOS smart card from you card issuer** that already holds your certificate. In these cases, you don't need to request a certificate and you can skip this section.

1. Install KOBIL Smart Key and your smart card terminal (see section 2.2).
2. Insert your TCOS smart card into your smart card terminal.
3. Start your Netscape Communicator
4. Surf to a certification authority of your trust, for example:
   - TeleSec Trustcenter (Germany): www.telesec.de
   - TC Trustcenter (Germany): www.trustcenter.de
   - Verisign (USA): www.verisign.com
5. Most of these certification authorities offer free trial certificates (often also called *Digital ID's*). You may choose a trial certificate, but note that this kind of certificates does not offer a high security level.
6. Enter some data that are required for your certificate (depending on the certification authority), for example:

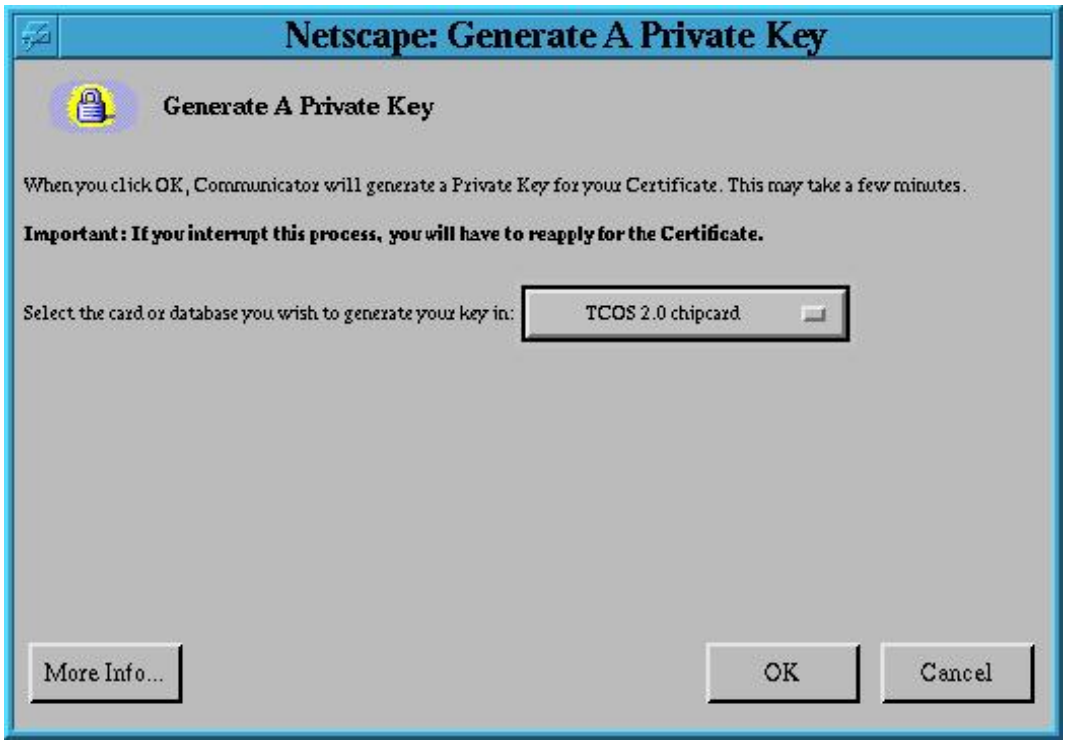
Netscape: Generate A Private Key
Generate A Private Key
When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.
Important: If you interrupt this process, you will have to reapply for the Certificate.
Select the card or database you wish to generate your key in:
TCOS 2.0 chipcard
More Info...
OK
Cancel

Figure 6.1: Key Generation Window

- Some personal data including your email address.
  It is really important that you enter your email address correctly (also case-sensitive!) as configured in you email account. Otherwise, you wont't be able to use your certificate!
- The key type and key length:
  - If you use a TCOS 2.0 smart card, choose **RSA, 1024 Bit**
  - If you use a TCOS 1.2 smart card, choose **RSA, 512 Bit**

  If you are not sure about your smart card, try **RSA, 1024 Bit**first.

7. Start the enrollment procedure by clicking the **Submit** button.

8. Now, Netscape will open a dialogue to ask in which **card or database** the new key will be stored as shown in figure 6.1. Choose **TCOS 2.0 chipcard** or **TCOS 1.2 chipcard**, depending on the card type you have.

9. **If your TCOS smart card has not yet a PIN**, you will have to initialize it now. Otherwise, this step is skipped.

   - First, you are asked for an **Administration Password**. This password is not supported by KOBIL Smart Key. You can just click **OK** to skip this dialogue without entering anything as shown in figure 6.2.
   - Now, you must enter the PIN of your TCOS smart card as shown in figure 6.3. **For a TCOS 1.2 smart card**, the PIN has to consist of **at least 4 digits** and **for a TCOS 2.0 smart card, it has to consist of at least 6 digits**.
     If you use a chipcard terminal with a keypad, you can enter there only digits! Thus, you should select a PIN that consists of digits only!

10. **If your TCOS smart card already has a PIN**, you are now asked to enter it. Depending on your chipcard terminal, you must enter the PIN either via your computer's keyboard (see figure 6.5) or via the chipcard terminal's keypad (*Secure PIN-entry*, see figure 6.4).

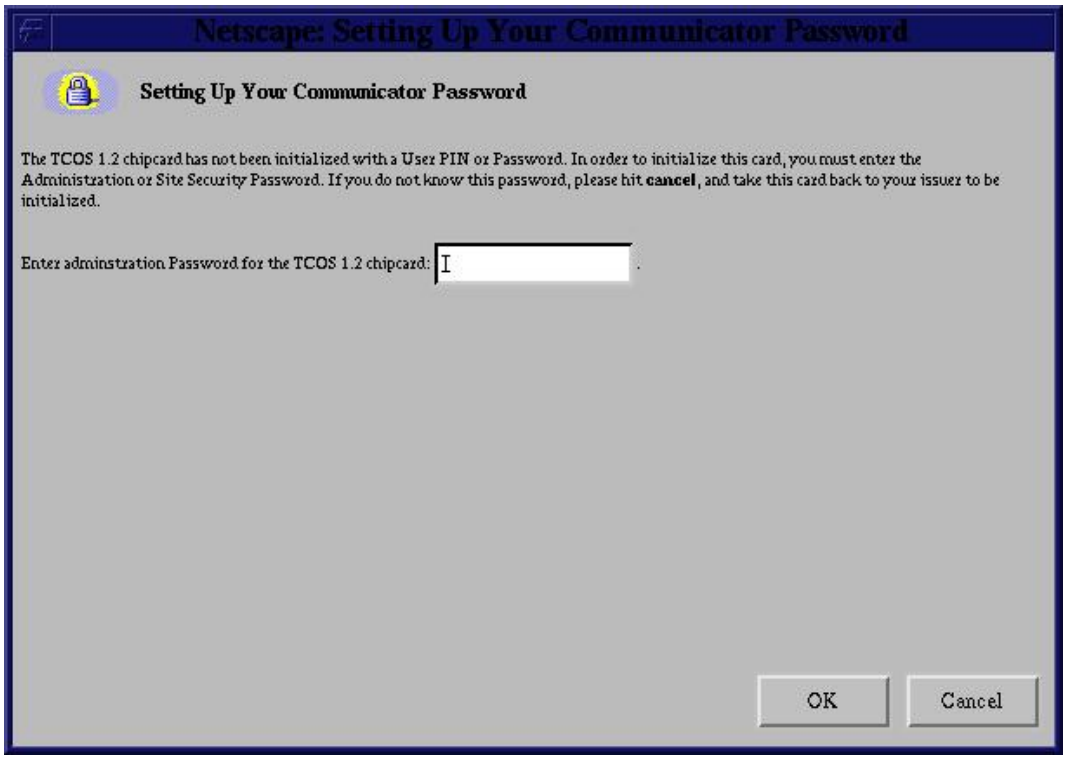
Netscape: Setting Up Your Communicator Password
Setting Up Your Communicator Password
The TCOS 1.2 chipcard has not been initialized with a User PIN or Password. In order to initialize this card, you must enter the Administration or Site Security Password. If you do not know this password, please hit cancel, and take this card back to your issuer to be initialized.
Enter adminstration Password for the TCOS 1.2 chipcard:
OK
Cancel

Figure 6.2: Enter Administration PIN Window (not supported)

Netscape: Setting Up Your Communicator Password
Setting Up Your Communicator Password
It is strongly recommended that you protect your Private Key with a Communicator password. If you do not want a password, leave the password field blank.
The safest passwords are at least 8 characters long, include both letters and numbers, and contain no words from a dictionary.
Password:
****
Type it again to confirm:
****
Important: Your password cannot be recovered. If you forget it, you will lose all of your certificates.
If you wish to change your password or other security preferences, choose Security Info from the Communicator menu.
More Info...
OK
Cancel

Figure 6.3: Initialise PIN Window

Figure 6.4: Secure PIN-entry via the chipcard terminal's keypad

Figure 6.5: PIN-entry via the Netscape dialogue

11. Now, your key pair is being generated on your computer and written to your TCOS smart card. This process is rather complex and may take a while, normally around 30 seconds[1].

12. Once the public key is successfully transmitted to the CA, you will either get your certificate immediately on the next web page or it will be sent to you by e-mail.

13. Follow your CA's instructions to import and install the certificate. If it does not install automatically, the installation procedure should be described by the CA. Finally your certificate will be written into your TCOS smart card.

14. Now, you can take a look on your new certificate under

    Communicator > Extras > Security Options > Certificates > Yours

    as shown in figure 6.6. For details see section 6.1.2.

15. In some cases, you have to import the **root certificate of your teustcenter**, if it is not yet present in the Netscape certificate manager. For details, see section 6.1.3.

Note that if you would like to use your certificate that was enrolled using Netscape also with Internet Explorer or Outlook, you will have to register it first using the CardManagement Tool. For details, see section 4.5.

Specifically note, that the number of certificates you can store on your smart card mainly depends on the available memory. We implemented an upper limit of 10 certificates, however with a 16KB TCOS 2.0 smart card, you usually can put a maximum of 6-8 certificates onto one card (depending on the length of the individual certificates). To remove a certificate, use the procedure described in section 6.1.2.

6.1.2 Managing Certificates

In this section, you'll learn how to manage your certificates using the Netscape certificate manager. You can open Netscape's certificate manager in two ways:

- In Navigator (web browser) using the button **Security**
- In Messenger (email client) over the menu

  Communicator > Extras > Security Options

The dialogue shown in figure 6.6 appears when you click on **Certificates**. Now, you have access to the Netscape certificate database where 4 individual types of certificates are stored:

1. Your own certificates (**Yours**)
2. Other people's certificates (**Others**)
3. Web server certificates (**Web-Sites**)
4. CA certificates (**Signers**)

[1]The quality of a cryptographic key depends heavily on real random input. Note that on Windows and OS/2 platforms, there are no bits that are really random, so it is much faster but possibly less secure. For maximal security, we recommend to do key generation on either Linux or Solaris.

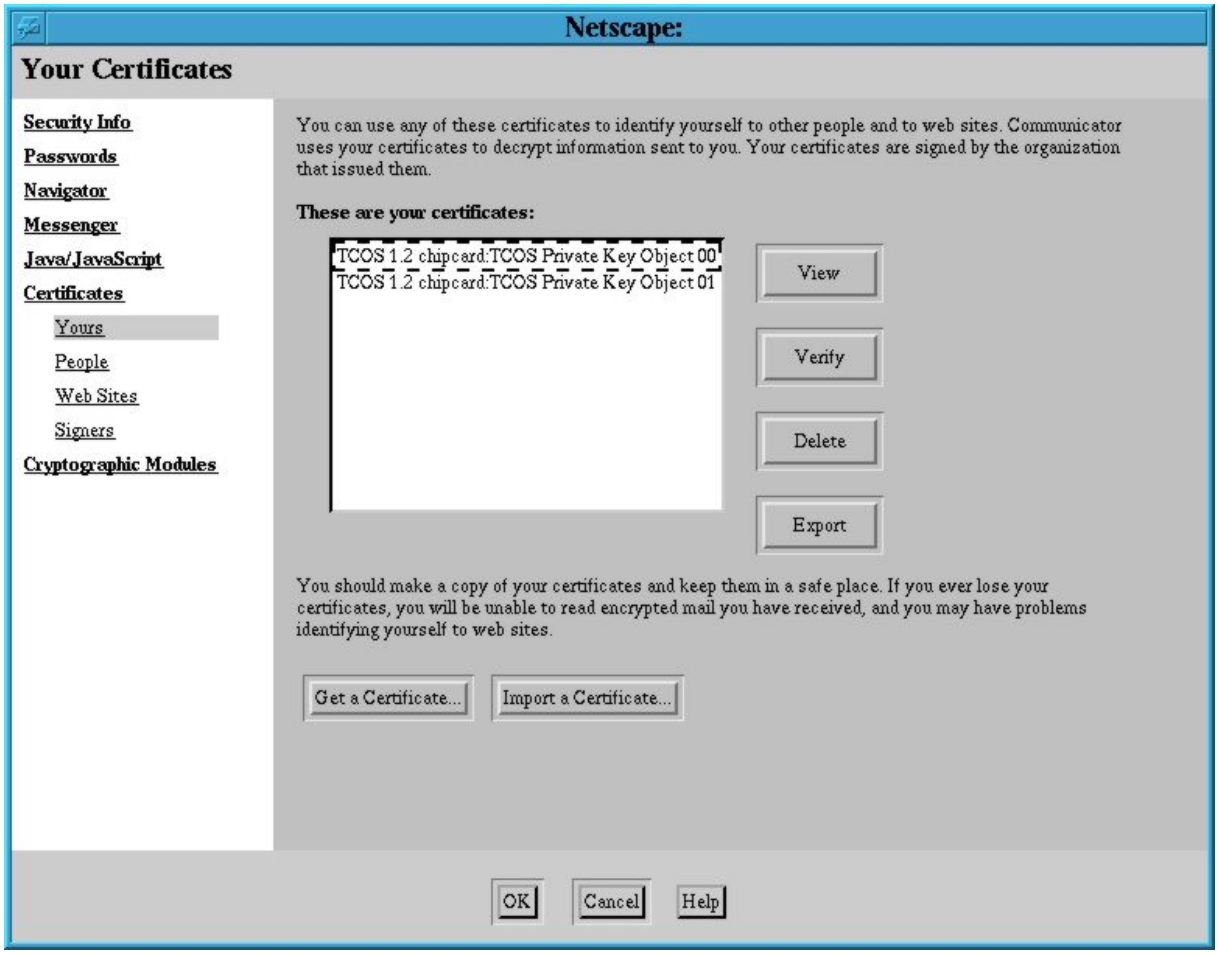
Netscape:
Your Certificates
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.
These are your certificates:
TCOS 1.2 chipcard:TCOS Private Key Object 00
TCOS 1.2 chipcard:TCOS Private Key Object 01
View
Verify
Delete
Export
You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.
Get a Certificate...
Import a Certificate...
OK
Cancel
Help

Figure 6.6: User certificates

Your own certificates (Yours)

Open the Netscape certificate manager (see section 6.1.2) and click

Certificates > Yours

Now, all your certificates are displayed as in figure 6.6. Your certficates are the ones where you possess the appropriate private key.

- The button **View** shows certificate details.
- The button **Verify** checks if the choosen certificate is valid.
- The button **Export** exports the choosen certificate with the corresponding private key. **Note that this function is not supported by KOBIL Smart Key, since you are not able to read out your private key from your TCOS smart card for security reasons.**
- You can delete the choosen certificate with the button **Delete**. **Be careful with deletion of your certificates, because after that, you cannot decrypt any messages encrypted with that certificate!**

Other people's certificates (Others)

Open the Netscape certificate manager (see section 6.1.2) and click

Certificates > Others

Now, all known certificates from other people are displayed as in figure 6.7.

- The button **View** shows certificate details.
- The button **Verify** checks if the choosen certificate is valid.
- You can delete the choosen certificate with the button **Delete**. **Be careful with deletion of other people's certificates, because after that, you cannot encrypt messages to this person, before you import it again (see section 6.1.4).**
- With the button **Search Directory** you can search for other people's certificates in a public directory service as described in section 6.1.4.

Web server certificates (Web-Sites)

Open the Netscape certificate manager (see section 6.1.2) and click

Certificates > Web-Sites

Now, all known certificates from web servers are displayed. They can be managed just like other people's certificates.

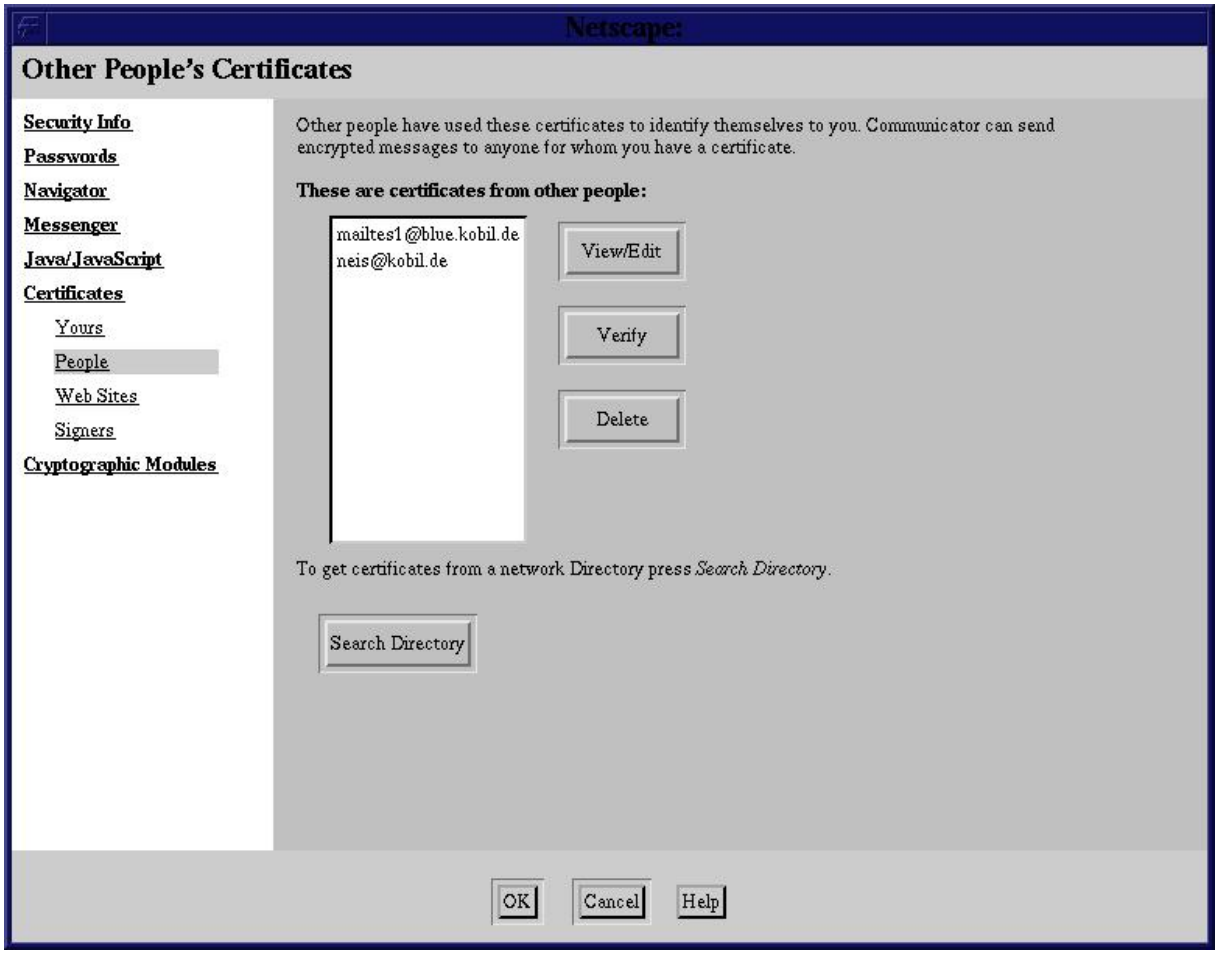

Figure 6.7: Other People's Certificates

CA certificates (Signers)

To make use of other peoples certificates, e.g. to verify their signatures, to send encrypted emails to them or to communicate via secured SSL connections, you need to know their certificate. However, if you try to obtain their certificates, anybody could intercept that connection and pass you whatever certificate he likes, so later somebody might intercept all the communication that you believe to be safe from such attacks.

To prevent this problem, certificates are required to be signed by some trustworthy instance, a so called certificate signer. That way you can verify the certificate's signature and know that nobody is giving you a wrong certificate - at least not without the active support of such a certificate signer.

Thus choosing the certificate signers that you accept is of critical importance. Netscape has a number of built-in certificate signers that you can see by clicking on

Security > Certificates > Signers

To know how to import a new CA certificate, see section 6.1.3.

6.1.3 Importing a new CA Certificate

Sometimes, you might feel the need to accept an additional certificate signer, for example if your bank is using a self-signed certificate for online banking.

In such cases, you can direct Netscape to the certificate signers site and install its certificate by clicking on a specific link. A sequence of dialogues will appear informing you that you are about to import a new CA certificate and that this is an important security operation. You will have to activate the purposes for which this CA will be enabled. Note that by default, no such purpose is active, so that you have to activate at least one purpose before you can use that CA certificate.

Note that you automatically get an implicit trust relationship to all users of the new certification authority when you import its CA certificate! You should inform yourself about the certification poliy of the new certification authority before importing its CA certificate.

6.1.4 Importing another User's Certificate

To send someone a secure mail, you need to add this person's certificate to your "Other People" certificates list (see figure 6.7). This can be done in two ways:

- You receive a signed e-mail from the other user. His certificate is included in each signed e-mail and will be imported automatically into the "Other People" certificate list.
- If you don't have received any signed e-mail from the other user yet, you can search for it in a public **Directory Service** which is kind of a phone book for certificates. You can search a directory service by clicking the button **Search Directory**. As search criteria, you can enter the other user's name or e-mail address. If you want to use any other than the pre-configured directory services, you will have to open your Netscape address book first via the menu

  Communicator > Adress Book

  and add the new directory service there by choosing the menu

  File > New Directory...

For the necessary parameter settings for your particular directory service, ask your system administrator.

You can also configure a directory service for **automatic search for certificates** of e-mail recipients by selecting the particular directory service in the menu

Edit > Preferences > Mail & News > Adressing

under **automatic address completion**.

6.1.5 Importing a Web Server's Certificate

If you surf on a secured web site (with the "*https://*"-prefix) whose server's certificate is not yet known under **Certificates > Web-Sites** and whose CA is not known under **Certificates > Signers**, a web server certificate import dialogue appears. In all other cases (web server's certificate is already known, web server's CA is already known), this dialogue will not appear.

During the dialogue you are advised that you are about to trust a new web server. You can either **accept this certificate forever (until it expires)** or **accept it only for this session**.

6.1.6 Changing the PIN of your TCOS Smart Card

On Windows plattforms, you can of course change the PIN of your TCOS smart card anytime using the CardManagement Tool (see section 4.5). This is also possible via Netscape, as the CardManagement Tool is not available on non-Windows plattforms.

The PIN, as all computer passwords can be changed. This should be done in regular intervals.

1. Open the Netscape security options dialogue

   Communicator > Extras > Security Options > Cryptographic Modules

   You will see figure 6.8.

2. Select the **KOBIL Smart Key** PKCS#11 module and click on **View/Edit**, so you will see figure 6.9.

3. **If you are using a smart card terminal without keypad**, click on **Change password** and enter the old and the new password in the dialogue as shown in figure 6.10.

4. **If your terminal has a keypad**, you will see the button **Initialise password** instead of **Change password**. Enter a sufficiently complicated password twice in the unneeded **Initialise password** dialog to get to the change password facility, where you can input old and new pin via the smart card terminal's keypad. This inconvenient step is necessary for technical reasons, since Netscape and the PKCS#11 specification do not know about secure PIN-entry.

   For a TCOS 1.2 smart card, the PIN has to consist of **at least 4 digits** and **for a TCOS 2.0 smart card, it has to consist of at least 6 digits**.

   If you use a chipcard terminal with a keypad, you can enter there only digits! Thus, you should select a PIN that consists of digits only!

6.2 Secure Web Sessions using Netscape Navigator

Secure Sessions rely on the SSL protocol (see section B.3.7, so all secure web sites are accessed using the **https://** prefix.

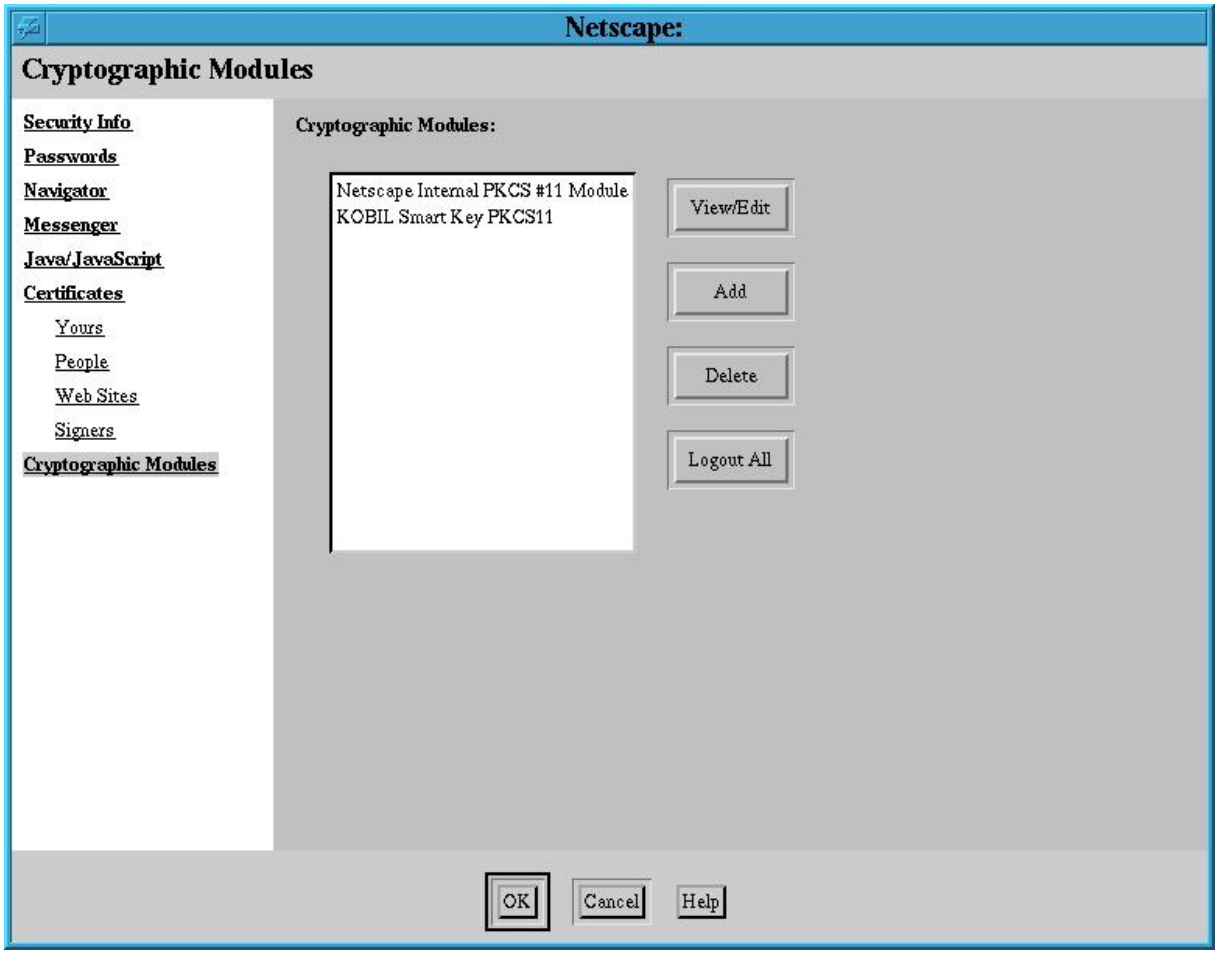

Figure 6.8: Cryptographic Modules

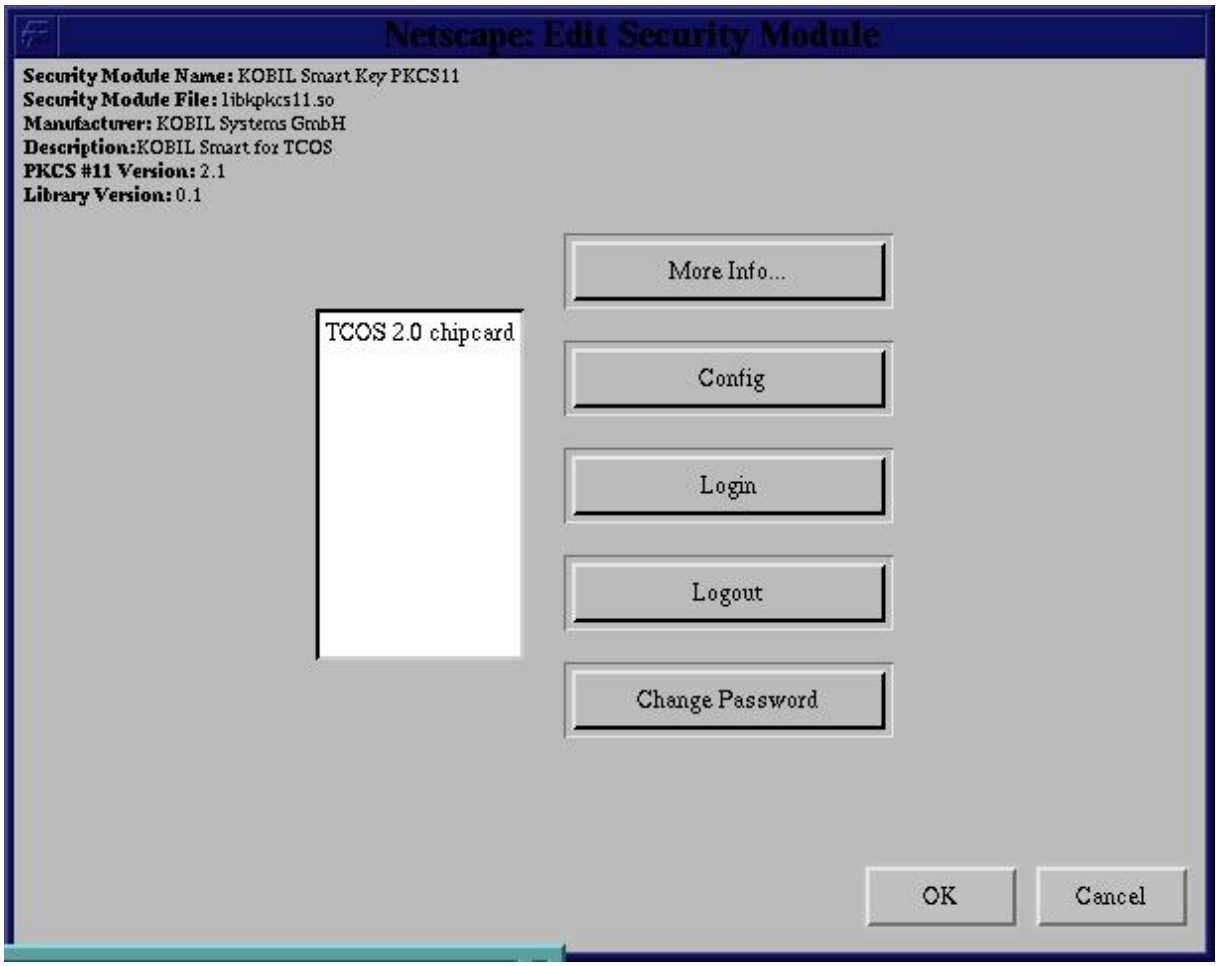

Figure 6.9: Cryptographic Module Details

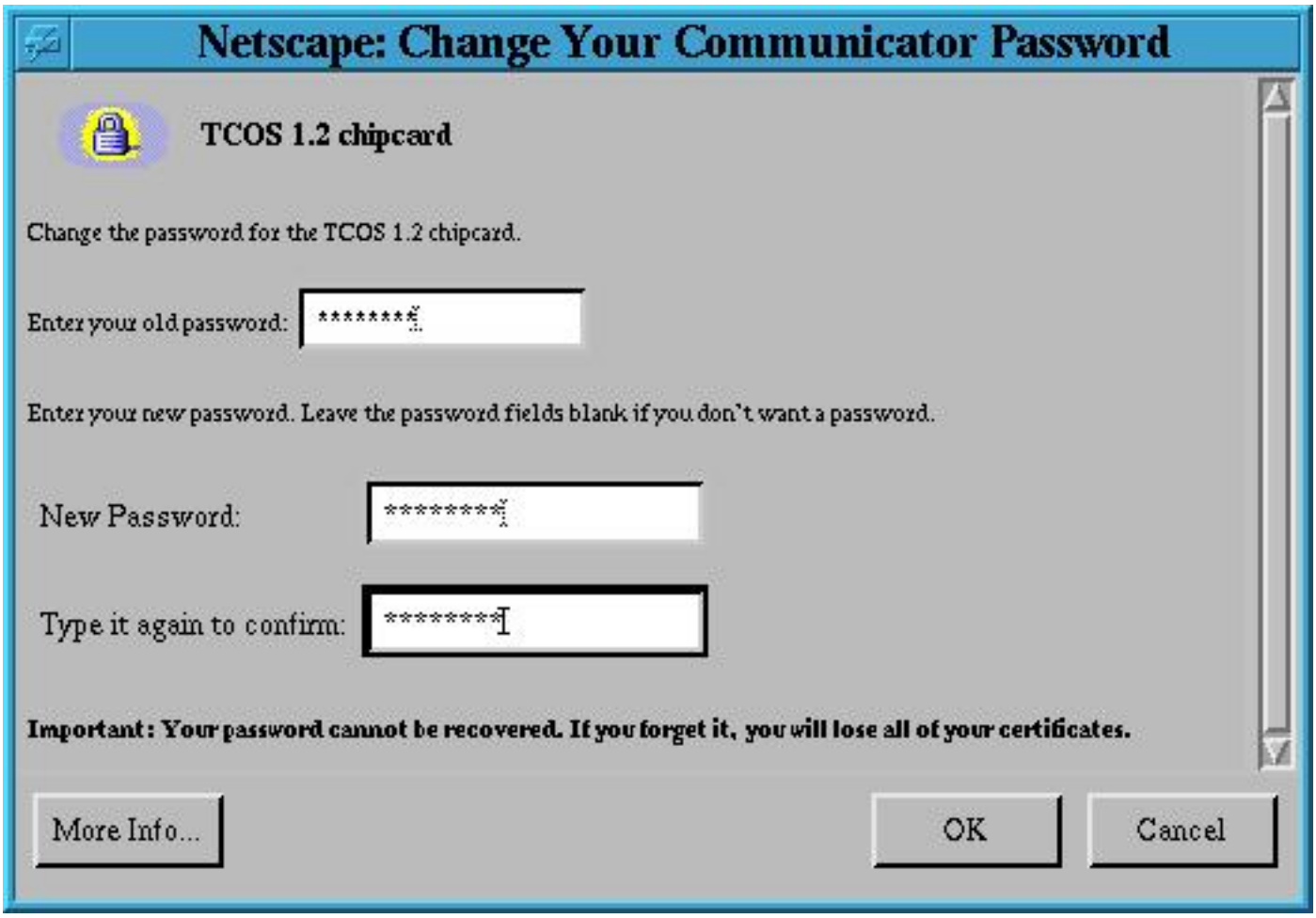
Netscape: Change Your Communicator Password
TCOS 1.2 chipcard
Change the password for the TCOS 1.2 chipcard.
Enter your old password:
Enter your new password. Leave the password fields blank if you don't want a password.
New Password:
Type it again to confirm:
Important: Your password cannot be recovered. If you forget it, you will lose all of your certificates.
More Info...
OK
Cancel

Figure 6.10: Changing the PIN using a smartcard terminal without keypad

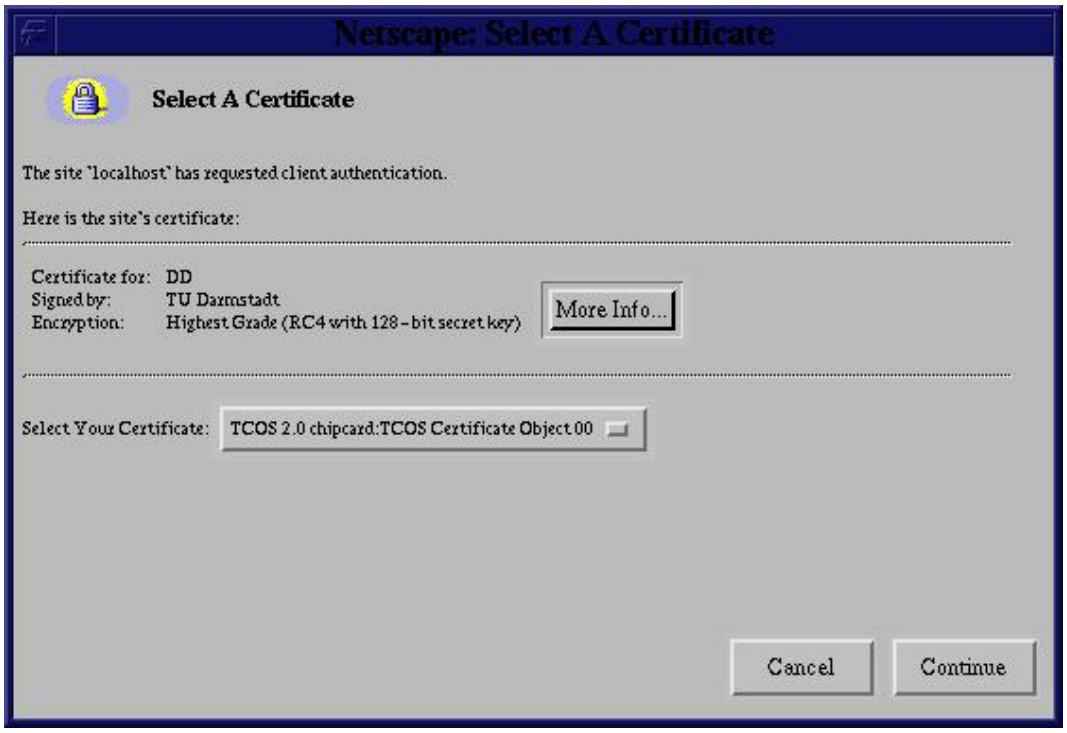

Figure 6.11: Selecting a Certificate

If your browser does already have the server's certificate (and if your browser has a certificate to confirm your identity - e.g. if it is stored on the smart card) a secure session will be initiated, otherwise, your access request will be rejected.

While initiating the secure session, you will have to choose the certificate to be used in confirming your identity in the screen shown in figure 6.11.

You can configure which default certificate to use by clicking **Security, Navigator** and choosing the desired certificate as **Certificate to identify you to a web site**.

Once the connection is establish, notice the padlock in the lower left-hand corner and in the middle of the tool bar. It should be in closed position, indicating that you are operating in secure mode. In insecure mode it would be opened, which would indicate that you are not using KOBIL Smart Key and not operating in secure mode.

Click **View, Page Info** to display the information regarding the server's certificate and the connection's encryption mode.

6.3 Secure E-mail Communication using Netscape Messenger

In this section, you'll learn how to secure your e-mails with Netscape Messenger using KOBIL Smart Key.

6.3.1 Choose your Certificate

To enable secure E-Mail, click on **Security, Messenger**(see figure 6.12). For some versions of Netscape, you need to choose the same global settings here that you also choose below, for the message specific options, for other version you might have to enable everything that you might want to enable in a mail.

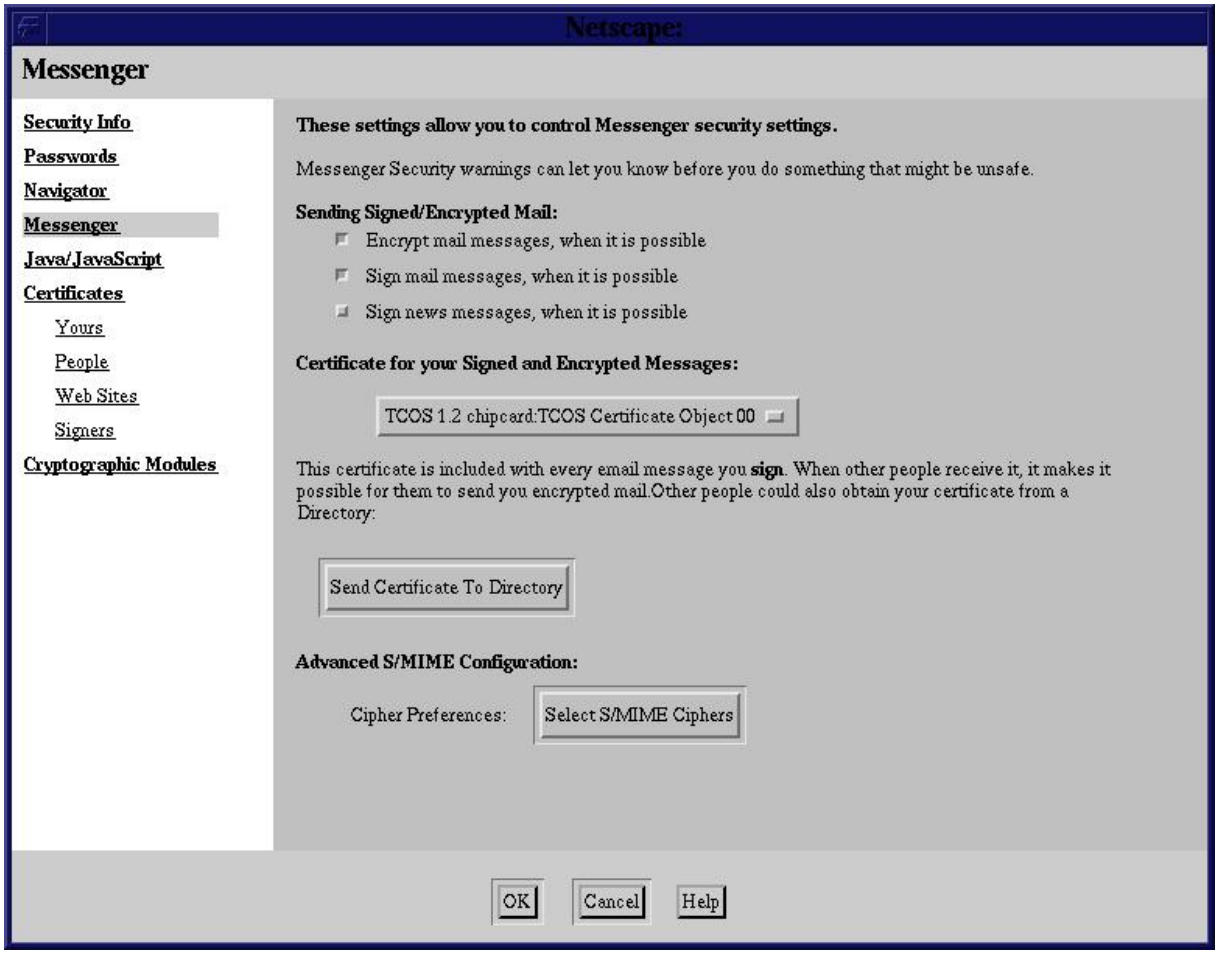
Netscape:
Messenger
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
These settings allow you to control Messenger security settings.
Messenger Security warnings can let you know before you do something that might be unsafe.
Sending Signed/Encrypted Mail:
Encrypt mail messages, when it is possible
Sign mail messages, when it is possible
Sign news messages, when it is possible
Certificate for your Signed and Encrypted Messages:
TCOS 1.2 chipcard:TCOS Certificate Object 00
This certificate is included with every email message you sign. When other people receive it, it makes it possible for them to send you encrypted mail.Other people could also obtain your certificate from a Directory:
Send Certificate To Directory
Advanced S/MIME Configuration:
Cipher Preferences:
Select S/MIME Ciphers
OK
Cancel
Help

Figure 6.12: Global Mail Options

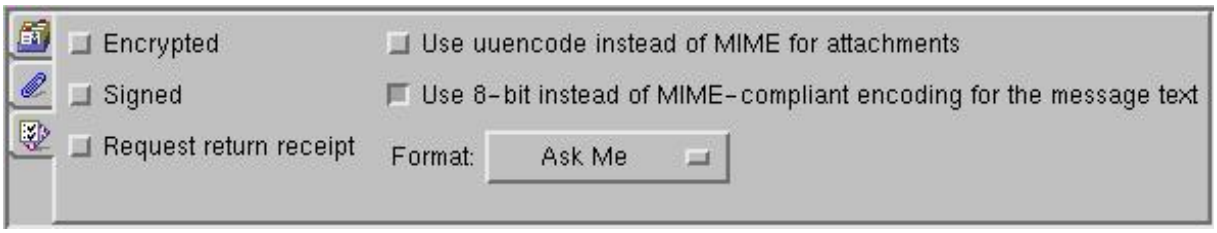

Figure 6.13: Sending Mail Options

Before you are ready to send an encrypted mail, you need to know the recipient's certificate (see above), if you want to send a message to several persons, you need to know a certificate for each of them, or your message will not be sent at all.

Once you receive a signed message from someone, the sender's certificate will be stored automatically, so you usually will not have to do this yourself. To view the list of certificates already known to your browser, click **Security, Certificates, People** (see figure 6.7). Your browser also automatically checks that the name in the e-mail address you are writing to corresponds to the name in the certificate.

In the same way, whenever you receive a signed message, your browser checks that the e-mail address of the sender matches his certificate.

In addition to globally setting/enabling security options you also can change this options in the mail header. If you click the icon for the sending options, the screen shown in figure 6.13 is displayed.

Depending on the your Netscape version, make sure, that the options you choose here are the same as those that are globally set or that at least you do not enable a feature that is disabled in the global options. If Netscape does not like the options you did choose, it will complain that you do not have a certificate although you do have one. If this occurs, remember to change either the global or the sending options in such a way that they match each other.

6.3.2 Sending secure E-Mail

After having chosen your e-mail certificate, you can start securing your e-mails as follows:

1. You can send your message in plain text - just as before.
2. You can sign your message. This will include your signature and your certificate into the e-mail. As the certificate contains your public key, anybody now can verify that the mail was send by you. This provides authenticity and integrity.
3. You can encrypt a message with the recipients public key. Thus the message can be read by the recipient only, as he is the only one able to decrypt your message. This provides confidentiality.
4. You can combine both encryption and signature to get confidentiality and authenticity and integrity.

6.3.3 Receiving secure E-Mail

If you receive a secured e-mail, Netscape shows a symbol representing the e-mail's status:

- **Signed:**This e-mail was signed and the signature was successfully verified. Click on the **Signed** image to look at details such as the signer's certificate.

- **Invalid Signature:** This e-mail was signed, but the signature was not successfully verified. Click on the **Invalid Signature** image to look at possible reasons why the verification failed.
- Enrypted:This e-mail was encrypted. Click on the **Encrypted** image to look at details such as the encryption algorithm.
- Invalid Encryption This e-mail was encrypted, but could not be decrypted. Click on the **Invalid Encryption** image to look at possible reasons why the decryption failed.
- Signed and Encrypted:This e-mail was signed and encrypted. Click on the **Signed and Encrypted** image to look at details such as the signer's certificate and encryption algorithm.

Appendix A

Problems and Solutions

In this chapter, typical problems using KOBIL Smart Key are identified and described. If you do not find the solution for your particular problem here, take a look in the web at **www.kobil.com** where you will find a FAQ list which is always kept up-to-date.

A.1 Connecting the chipcard terminal

- **During installation, the setup routine claims that the chipcard terminal could not be found:**
  - Make sure that your chipcard terminal is correctly connected to your computer. If you have a model with serial interface (COM-port), the keyboard adapter or the KOBIL external power supply has to be conntected, too!
  - Chipcard terminals with Plug-and-Play capabilities occur in the Windows device manager.
- **My PC has no PS/2 port for the keyboard adaptor:**
  - You can order from KOBIL a cable set for older AT-like keyboard interfaces (5-pin plug), take a look in the web at www.kobil.com

A.2 KOBIL Smart Key for Microsoft-Applications

- **Certificate enrollment fails:**
  - Make sure that your Certification Authority (CA) supports CSP's correctly.
- **Outlook refuses to send a signed mail:**
  - Make sure that you have already a certificate (see Section 4.3.1).
  - Make sure that your certificate is valid.
- **Outlook refuses to send an encrypted mail:**
  - Make sure that you have the recipient's certificate (see Section 4.1.5).
- **Outlook cannot decrypt a mail that has been sent to you:**
  - If the mail was not encrypted with your certificate, you cannot decrypt it.
  - If the mail was encrypted with a certificate that you have deleted on your card, you are not able to decrypt it.

- **Authentication to a secure Web site fails:**
  - The secure web server may not accept the Certification Authority (CA) where you enrolled your certificate.
  - Your certificate may be not be valid or revoked.
- **Windows 2000 smartcard logon doesn't work:**
  - Make sure that a PC/SC driver is installed for your chipcard terminal. Your KOBIL chipcard terminal must appear in the device manager under *Smart Card Readers*.
  - You need a special smartcard login certificate on your chipcard (see section 5.3). Other certificates will not work.
  - Windows 2000/XP smartcard login requires a Windows 2000 / 2003 Server acting as a domain controller.
  - Just after installing the Windows 2000 CA, it can take some time until the new CA root certificate and the certificate revocation list are distributed to the clients. The Windows group policy interval is 8 hours by default. Check first, if you can logon at your server using your smartcard (it may be necessary to change the domain controller's local security policy to allow normal users to logon).

A.3 KOBIL Smart Key PKCS#11 module for Netscape

- **Netscape refuses to send a signed mail:**
  - Make sure that you have already a certificate (see Section 6.3).
  - Make sure that your certificate for signed and encrypted mails is correctly set (see Section 6.12).
  - Make sure that your certificate is valid. Chose your certificate as shown in figure 6.6 and click on the **Verify** button.
- **Netscape refuses to send an encrypted mail:**
  - Make sure that you have the recipient's certificate (see Section 6.1.2).
- **Netscape cannot decrypt a mail that has been sent to you:**
  - If the mail was not encrypted with your certificate, you cannot decrypt it.
  - If the mail was encrypted with a certificate that you have deleted on your card, you are not able to decrypt it.
  - If you are running an older version of Netscape, you might not have full encryption strength. In that case, you should use the latest Netscape version or install **Fortify** (see www.fortify.net).
- **Authentication to a secure Web site fails:**
  - The secure web server may not accept the Certification Authority (CA) where you enrolled your certificate.
  - Your certificate may be not be valid or revoked.
  - If you are running an older version of Netscape, you might not have full encryption strength. In that case, you should use the latest Netscape version or install **Fortify** (see www.fortify.net).

Appendix B

Cryptographic Basics and Standards

B.1 Security Objectives

Confidentiality Protection from disclosure to unauthorised persons who may try to listen to communication or to steal some information.

Integrity Maintaining data consistency. Nobody except the originator can change the information while it is stored somewhere or transfered in an insecure media like the Internet.

Authentication (Non-repudiation / Access control) Assurance of identity of a person or an originator of data. The originator of some data cant deny it later. Unauthorized persons are kept out.

B.2 Terms and Basics

Cryptography is the science of keeping information secure. Cryptographic systems usually consist of two implemented processes: encryption and decryption.

Encryption is the process of transforming a message (the plaintext) into another message (the ciphertext) such that it is computationally infeasible to derive the plaintext data by reversing the process without knowledge of secret parameters. Many cryptographic algorithms mathematically combine input plaintext data and an encryption key to generate ciphertext data.

Decryption is the reverse process of encryption and transforms the ciphertext data back into the original plaintext data by using a complex function and a decryption key. One of the goals of cryptography is to raise the cost of guessing the decryption key beyond what is practical. The algorithm type and the key length are the most important measures against predictability of the key.

Cryptography has nothing to do with obscurity. Cryptographic algorithms and protocols should be conform with standards to support interoperability. Using non-published algorithms is contraproductive to compatibility. Moreover, cryptography is not about hiding algorithms, but it is about designing strong algorithms and secure mechanisms. Security and interoperability must both be achieved in years by building and testing very well-known algorithms, mechanisms and protocols. Security should be obtained only by storing the keys in a secure way and by making algorithms so strong that they are impractical to break.

B.3 Standards

B.3.1 Data Digestion Algorithms

Data Digestion Algorithms are not used for encryption or decryption. The main purpose of these algorithms is to produce a unique "fingerprint" (typically 16 or 20 bytes in length) of the original data.

Digestion algorithms are also called "one-way hash functions", because it is computationally infeasible to recover the original data from its digest or even to find some other data which will produce the same digest. Ideally, each digest is unique and every bit is influenced by every bit of its input data. These algorithms are used together with other types of algorithms to supply digital signature processes (see below). The most common digestion algorithms are MD5, RipeMD and SHA1. Figure B.1 illustrates the data digestion process.

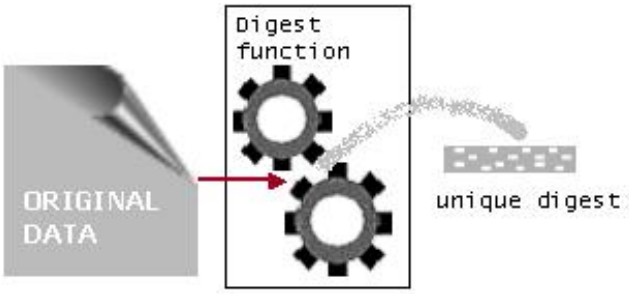

Figure B.1: Data Digest scheme

B.3.2 Symmetric Encryption Algorithms

With these type of algorithms, the same key (the so-called "session key") is used to encrypt and the decrypt the message. They are also known as "session key algorithms". Figure B.2 illustrates the symmetric encryption process.

The main advantage of symmetric algorithms is their speed of data encryption and decryption. The main weakness is the key management. Both sender and receiver must have the same secret session key which must be transferred securely. It is convenient and secure to transfer session keys by using public key algorithms. The most common session key algorithms currently are triple DES, RC2 and RC4.

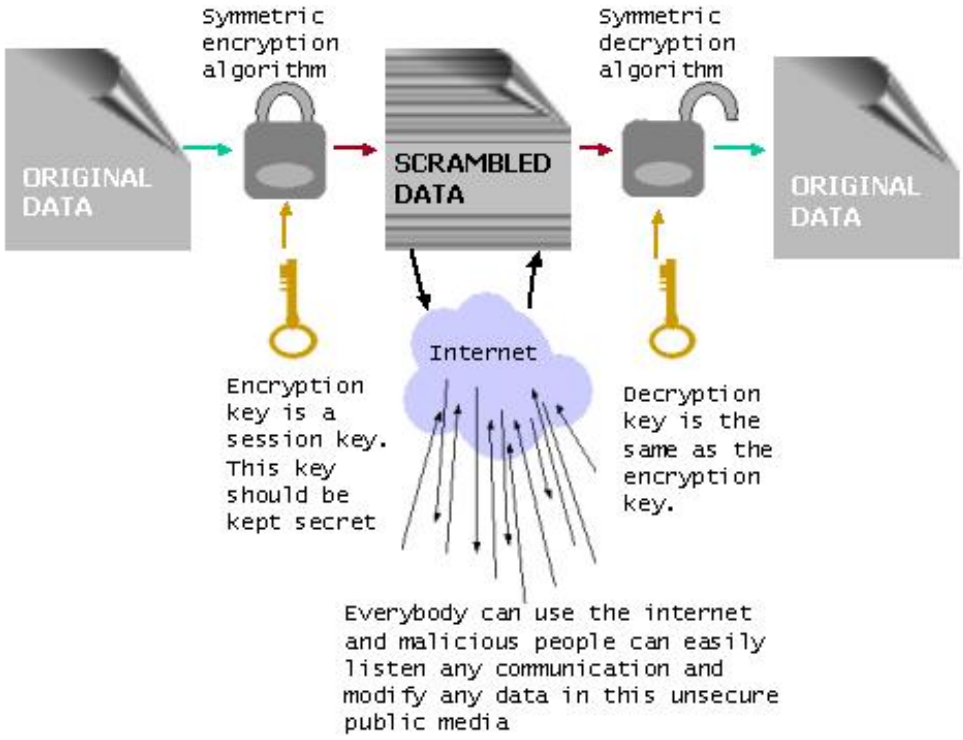

Figure B.2: Symmetric Algorithm

B.3.3 Public Key Algorithms

Properties

With these algorithms, encryption and decryption keys are different. Each user has at least one key pair consisting of two keys. One is kept secret, so it is called a "private key", and the other one is open, which is called "public key". Private keys are unique for each user and they are never transferred to other people.

If someone needs to send a data to you, he needs your public key. He encrypts data with your public key and no one except you can decrypt the scrambled data using your private key. The transfer (or distribution) of your public key is secured by the help of "trusted authorities". Such a trusted authority will provide you a certificate for your public key. This means that they provide a packet of data containing both your public key and the trusted authority's assurance that this is really your public key. Figure B.3 illustrates the usage of public key process for a secure data transfer.

The main advantage of the public key algorithms is the secure key distribution. Their main disadvantage is the slow processing speed for encryption and decryption of large data. Because of this slowness, public key algorithms are used with together with symmetric session key algorithms to supply the necessary speed. To support confidentiality, public key algorithms are used to wrap and unwrap the session keys (for a secure session key transfer). To support both integrity and authentication, public key algorithms are used to sign and verify the output of data digestion algorithms. The most common public key algorithm is RSA.

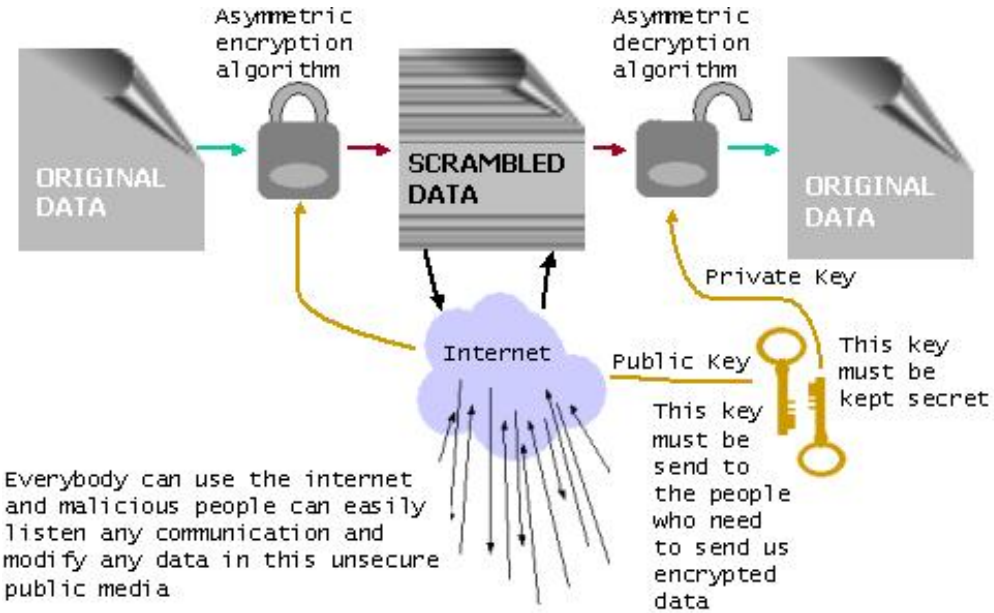

Figure B.3: Asymmetric Algorithm

Wrap Session Key

Bulk data is encrypted with a session key to supply fast speed. The encryption session key must be sent to the recipient for decryption. For a secure transfer, the session key is encrypted with the public key of the recipient. No one except the recipient can recover the session key, because the private key of the recipient is needed to decrypt the scrambled session key. Encrypted bulk data and the scrambled session key are merged to form a digital envelope. Someone who wants to recover the original data must recover the session key first (see figure B.4).

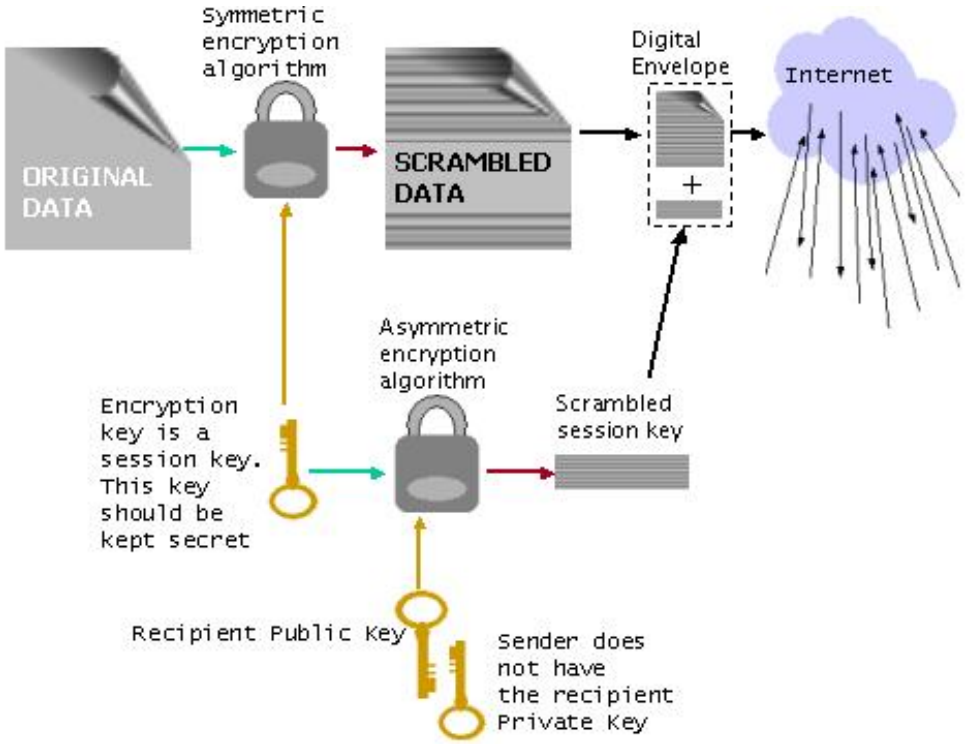

Figure B.4: Wrap Session Key

Unwrap Session Key

The recipient of the digital envelope detaches the scrambled session key from the encrypted bulk data. First, the scrambled session key is decrypted with the private key of the recipient. Second, bulk data is decrypted with the recovered session (decryption) key as shown in figure B.5.

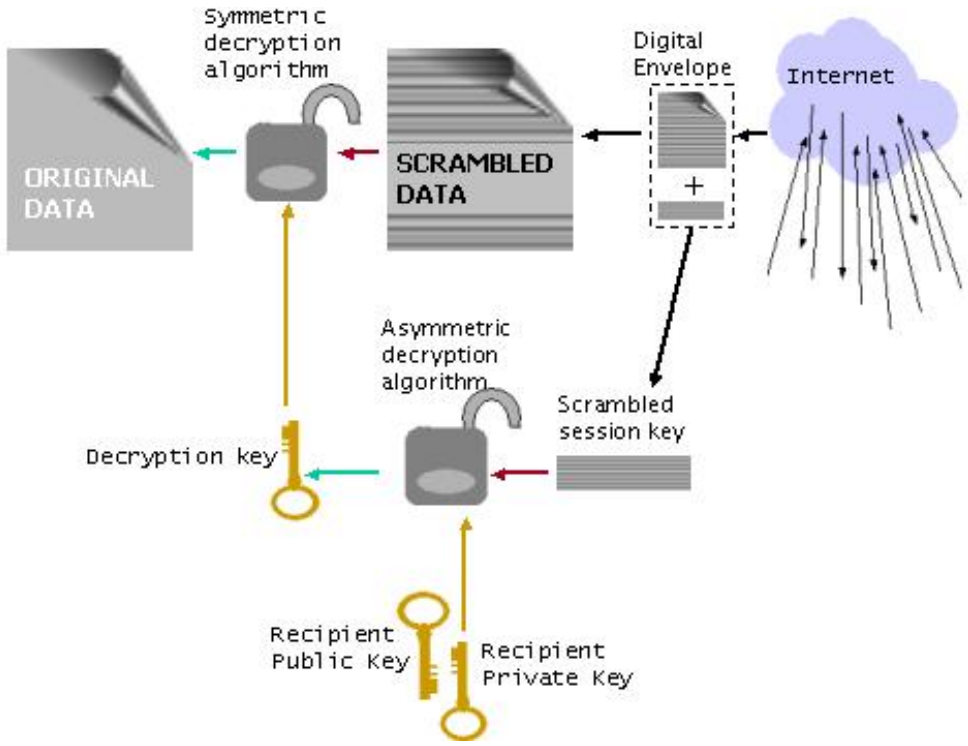

Figure B.5: Unwrap Session Key

Digital Signatures

Digital signatures are needed for the authentication of identities. A digital signature binds an individual to unique data. That's why there are two inputs of the signing process: first, the data itself and second, the private key of the signing individual.

Digestion algorithms are used to reduce the size of the bulk data because of the slowness of the public key algorithms. First, the message is digested and then the unique digest is encrypted with the originator's private key. Output is the signature. Anybody can decrypt this signature, because anybody can get the corresponding public key of the sender. The result of decryption is the unique digest and it is practically infeasible to find another message with the same digest.

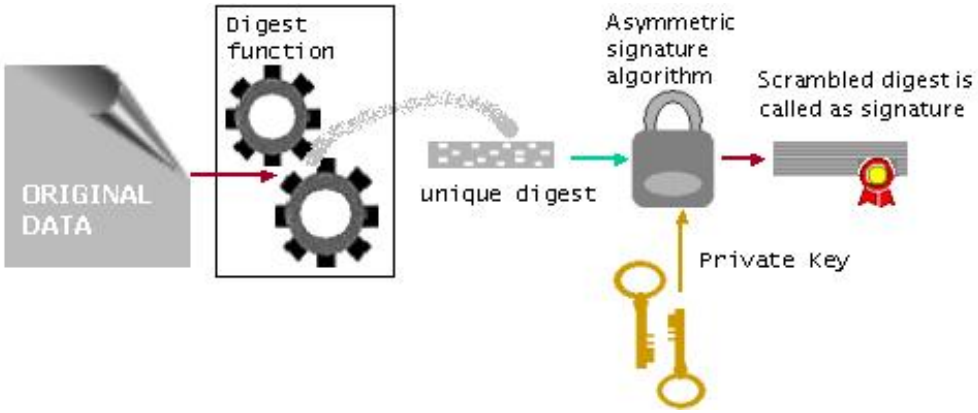

Figure B.6: Signature Creation

Verification of Digital Signatures

To verify a digital signature, someone needs both the signature and the input data. A recipient of the signature decrypts it with the sender's public key to recover the data digest. The recipient also digests the input data to get the original data digest. If the recovered data digest is the same as the original digest, the signature is correct. Otherwise, the sender is not the person who he claims to be or the original data was modified on its way. Digital signatures support both authentication and integrity. For confidentiality, digital signing process is combined with the encryption process of session keys and the wrap operation of public keys.

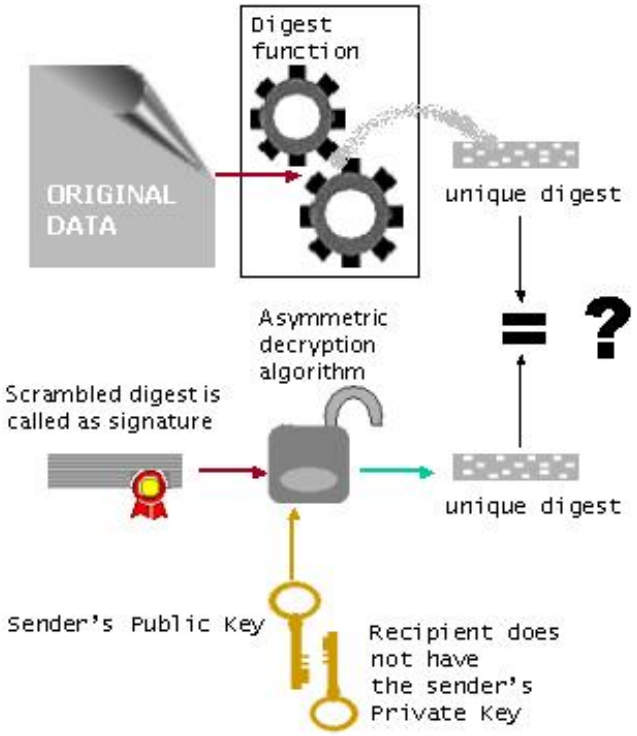

Figure B.7: Signature Verification

B.3.4 Digital Certificates

A certificate is a set of data that includes a public key and other owner- specific information to identify an entity. The certificate owner has the corresponding private key. Certificates are issued by certification authorities (CA) which are trusted organisations. Each certificate is protected by a signature that is created by a CA. Certification authorities and certificates make public key distribution secure. Secure storage and usage of a certificate and its corresponding private key is the problem of its owner. KOBIL Smart Key helps certificate owners with this problem by presenting a hardware based security system that uses smart cards.

The most widely accepted standard for digital certificates is defined by International Telecommunications Union's ITU-T X.509 standard. A X.509v3 certificate includes the following data fields:

- Version
- Certificate's serial number
- Signature algorithm ID
- Issuer name
- Expiration date
- User name
- User public key information

- Issuer unique identifier (optional)
- User unique identifier (optional)
- Extensions (optional, contain certificate usage instructions)
- Issuer's signature over the fields above

B.3.5 Certificate Authorities

A certificate authority (CA), also called "trust center", is a trusted organisation that issues public key certificates. A CA acts as a guarantor of the binding between the subject's public key and the subject's identity information that is contained in the certificates it issues.

The typical process of getting and using a certificate goes something like this (the user is called *Alice*[1] in this example):

1. Alice creates a cryptographic key pair, consisting of a private and a public key.
2. Alice creates a certificate request that contains her name, her public key, and perhaps some additional information.
3. Alice signs her certificate request with her new (corresponding) private key.
4. Alice sends the signed request to a CA.
5. The CA creates a data set from Alice's request.
6. The CA signs the data set with its private key.
7. The CA forms a certificate with the data set and its signature.
8. The CA returns the certificate to Alice who is now the owner of the certificate.

To give a real meaning to this process, the CA would of course need to make sure that Alice really is Alice (and not e.g. Bob claiming to be Alice). This however causes additional costs and actions in real life, so this is something which a pure Internet service cannot provide. However, there are companies offering that type of service.

Today's most popular browsers and e-mail programs know the certificates of very well known and more or less trusted CAs. So people can easily verify the signatures of many CAs. This helps people to decide whether a certificate and its content is trustworthy or not. If a certificate is signed and issued by an unknown CA and your browser does not have the public key of that CA, then your browser gives a warning and asks whether to proceed or not.

The typical certificate distribution and verification between users:

1. Alice sends her certificate to Bob to give him access to her public key. This is typically achieved by sending a signed, but not encrypted, message to Bob.
2. Bob verifies the signature of Alice's certificate by using the CA's public key. If the signature proves to be valid, he accepts the public key in the certificate as Alice's public key. Today's browsers and e-mail programs handle verification automatically.

[1] In cryptographic protocols, the users are often called *Alice* and *Bob*

B.3.6 Smart Cards and Readers

Smart cards are credit card-sized devices with integrated circuit chips (ICC) on them. They have their own security mechanisms to lock themselves against physical, electrical and chemical attacks. When private keys are loaded, they never leave the smart card and a PIN code protects the key usage. Smart Cards are easy to use. They can fit in a wallet and can be easily carried.

Terminals (often called readers, although they are usually able to write as well) are the devices which enable communication between a smart card and a computer. Smart card terminals can be connected to computers via serial or USB ports. An important advantage of some (more expensive) terminals is the secure PIN entry option, which is possible if a reader has its own keypad, display and special software on it.

Figure B.8: Smart Card Terminals

B.3.7 Secure Socket Layer(SSL)

Secure Sockets Layer (SSL), developed by Netscape Communications, is a standard security protocol that provides security and privacy on the web. The protocol allows client/server applications to communicate securely. This is achieved by an online, interactive process which handles secure and authentic exchanges of some random data which is finally used to generate the session key on both sides. SSL uses both public key and session key algorithms. Work flow of the SSL is illustrated in figure B.9. In many cases, client authentication is optional, since clients may not have certificates.

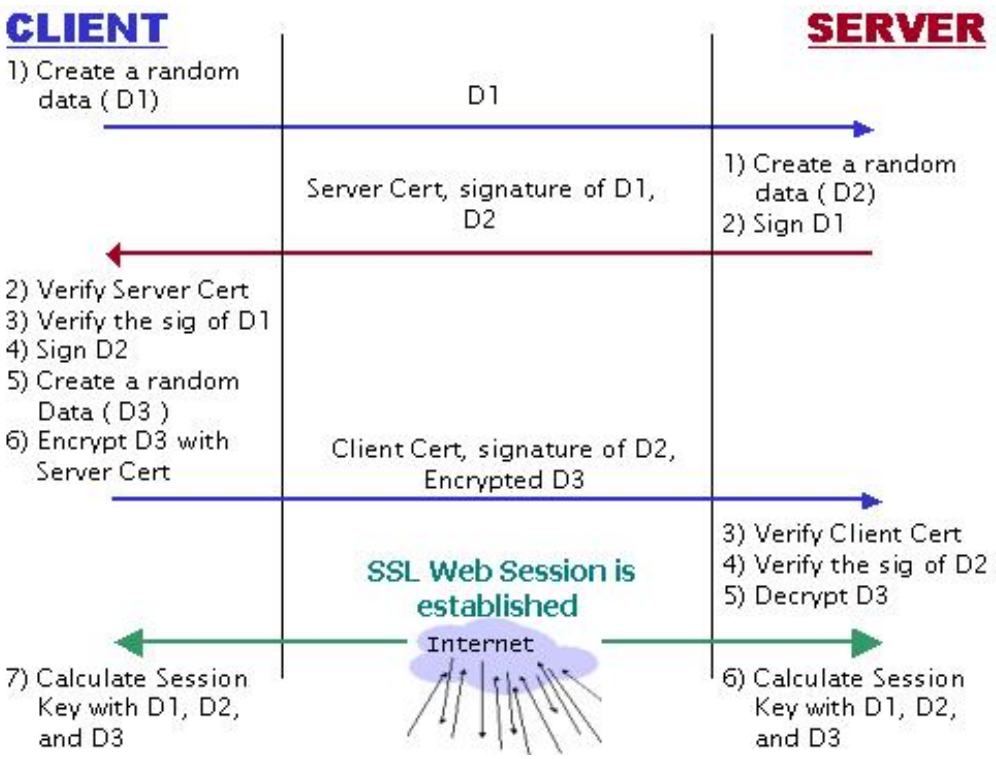
CLIENT
SERVER
1) Create a random data (D1)
D1
1) Create a random data (D2)
2) Sign D1
Server Cert, signature of D1, D2
2) Verify Server Cert
3) Verify the sig of D1
4) Sign D2
5) Create a random Data (D3)
6) Encrypt D3 with Server Cert
Client Cert, signature of D2, Encrypted D3
3) Verify Client Cert
4) Verify the sig of D2
5) Decrypt D3
SSL Web Session is established
Internet
7) Calculate Session Key with D1, D2, and D3
6) Calculate Session Key with D1, D2, and D3

Figure B.9: Secure Socket Layer

B.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME)

Secure Multipurpose Internet Mail Extensions (S/MIME) is an open protocol standard developed by the RSA Laboratories that provides encryption and digital signature functionality to Internet e-mail. S/MIME uses public key cryptography standards to define e-mail security services. S/MIME includes offline processes.

The sender's process is illustrated in figure B.10, the recipient's process is illustrated in figure B.11.

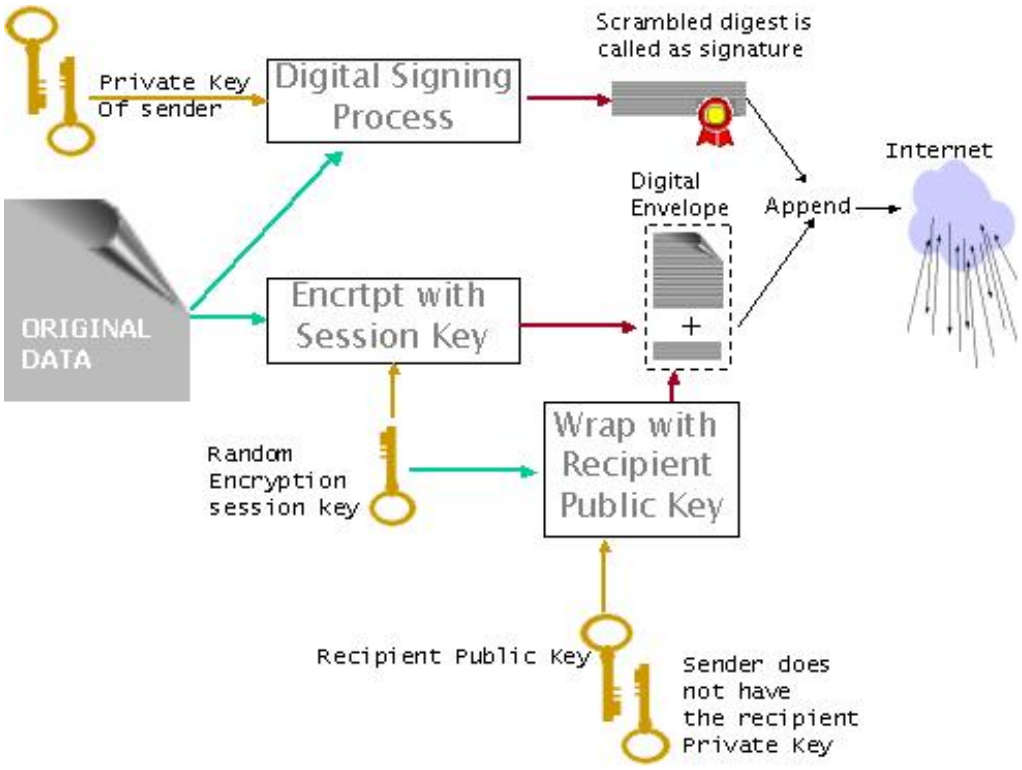

Figure B.10: Sender Process in S/MIME

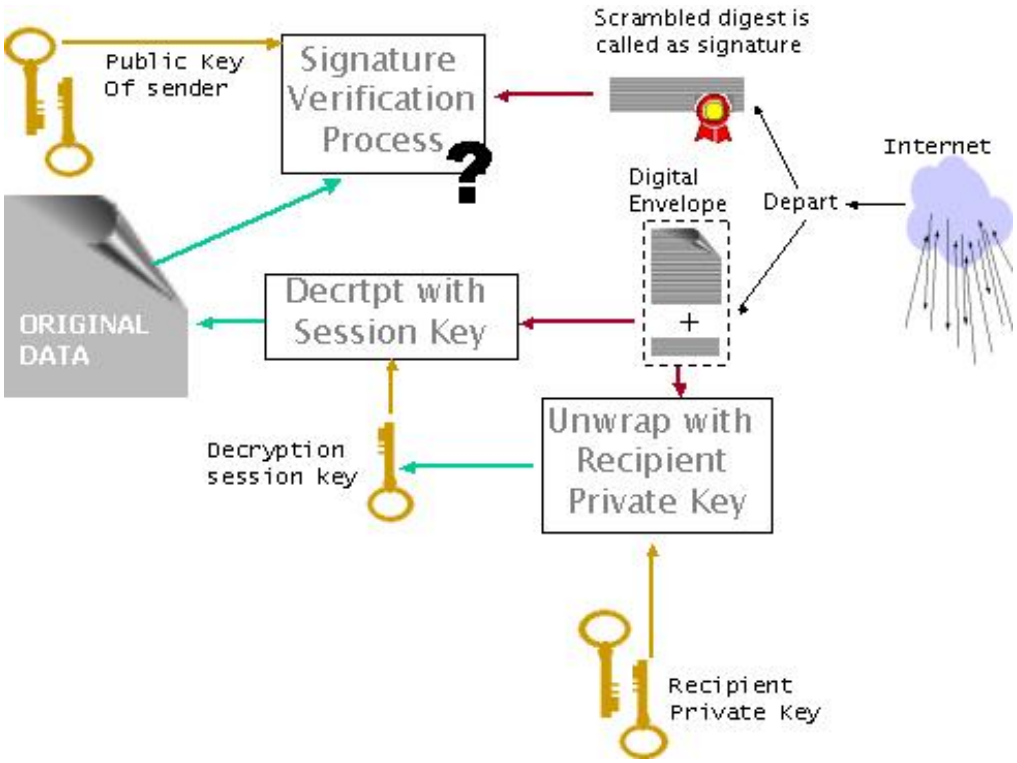

Figure B.11: Recipient Process in S/MIME

Appendix C

Glossary

Algorithm A mathematical formula used to perform computations that can be used for security purposes.

Authenticate To determine the identity of the entity that signed a message (entity authentication), or to verify that a message was not altered (data authentication).

Certificate Authority (CA) An entity with the authority and methods to certify the identity of one or more parties in an exchange (an essential function in public key crypto systems).

Cryptography The art and science of transforming confidential information to make it unreadable to unauthorised parties.

Data Encryption Standard (DES) A block cipher that encrypts data in 64-bit blocks. DES is a symmetric algorithm that uses the same algorithm and key for encryption and decryption. Developed in the early 1970s, DES is also known as the DEA (Data Encryption Algorithm) by ANSI and the DEA-1 by ISO.

Decryption The process in which ciphertext is converted to plaintext.

Digital Certificate A digital certificate provides identification for secure transactions. It consists of a public key and other data about the user, all of which is digitally signed by a Certificate Authority. It is a condition of access to secure e-mail or to secure Web sites.

Digital Signature A data string produced using a public key crypto system to prove the identity of the sender and the integrity of the message.

Encryption A cryptographic procedure whereby a legible message is encrypted and made illegible to all but the holder of the appropriate cryptographic key.

Internet Explorer (IE) Microsoft Internet browser.

Inter-operability The ability of products manufactured by different companies to operate correctly with one another.

Key A value that is used with a cryptographic algorithm to encrypt, decrypt, or sign data. Secret key (symmetric) crypto systems use only one secret key. Public key (asymmetric) crypto systems rely on a matched key pair to encrypt and decrypt data.

Key Length The number of bits forming a key. The longer the key, the more secure the encryption.

MD5 A hashing algorithm that creates a 128-bit hash value, which is twice the size of the block (64 bits).

Personal Computer/Smart Card (PC/SC) Standards that define the interface between smart cards and smart card readers.

Public Key Cryptography Standards (PKCS) A cryptographic system that uses two different keys (public and private) for encrypting data. The most well-known public key algorithm is RSA.

Rivest, Shamir, Adleman (RSA) Developers of the RSA public key crypto system and founders of RSA Data Security, Inc.

Secure Hash Standard (SHA) A standard designed by NIST and NSA. This standard defines the Secure Hash Algorithm (SHA-1) for use with the Digital Signature Standard (DSS).

Secure Sockets Layer (SSL) Security protocol used between servers and browsers for secure Web sessions.

SSL Handshake The SSL handshake, which takes place each time you start a secure Web session, identifies the server. This is automatically performed by your browser.

Secure/Multipurpose Internet Mail Extensions (S/MIME) Standard offline message format for use in secure e-mail applications.

Uniform Resource Locator (URL) Web address.